Standardid, suunised ja protseduurid infosüsteemide auditeerimise ja juhtimise spetsialistidele

- **Kutse-eetika koodeks**
- **Infosüsteemide auditeerimise standardid, suunised ja protseduurid**
- **Infosüsteemide juhtimise spetsialistide standardid**

Seisuga 1. mai 2008

ISACA

See teos on "IS auditeerimise standardite, IS auditeerimise protseduuride ja IS auditeerimise suuniste" ingliskeelse redaktsiooni tõlge, mille on Infosüsteemide auditi ja juhtimise assotsiatsiooni (ISACA) loal eesti keelde pannud ISACA Eesti haruühing. Eesti haruühing võtab ainuvastutuse tõlke täpsuse ja tõepära eest.

This Work is translated into Estonian from the English language version of the *IS Auditing Standards, IS Auditing Procedures and IS auditing Guidelines* by the Estonia Chapter of The Information Systems Audit and Control Association (ISACA) with the permission of ISACA. The Estonia Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

Lahtiütlus IS auditeerimise standardite kohta

ISACA on teose "IS auditeerimise standardid, IS auditeerimise protseduurid ja IS auditeerimise suunised" kavandanud vastuvõetava sooorituse minimaalse tasemena, mis on vajalik ISACA infosüsteemiaudiitorite kutse-eetika koodeksis sõnastatud kutsealaste kohustuste täitmiseks. ISACA ei väida, et selle toote kasutamine tagab eduka tulemuse. Seda väljaannet ei tohiks vaadelda sellisena, mis sisaldaks mingeid õigeid protseduure ja teste või välistaks muid protseduure ja teste, mis on mõistlikult suunatud samade tulemuste saamisele. Iga konkreetse protseduuri või testi õigsuse määramisel peaks meetmete spetsialist rakendama oma kutsealast otsustusoskust konkreetsetele juhtimisolukordadele, mis tulevad ette konkreetsetes süsteemides või infotehnoloogilistes keskkondades.

ISACA has designed the Work *IS Auditing Standards, IS Auditing Procedures and IS Auditing Guidelines* as of the minimum level acceptable performance required to meet the professional responsibilities set out in the ISACA *Code of Professional Ethics* for IT auditors. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the security and control professional should apply his/her own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

IS auditeerimise standardite avaldamine ja autoriõigus

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 USA

Telefon: +1 847 253 1545

Faks: +1 847 253 1443

E-post: standards@isaca.org

Veebisait: *www.isaca.org*

Sisukord

Kutse-eetika koodeks

Information Systems Audit and Control Association®, Inc. (ISACA, Infosüsteemide Auditi ja Juhtimise Assotsiatsioon) esitab oma liikmete ja/või ISACA sertifikaadi omanike kutsealase ja isikliku käitumise suunamiseks käesoleva kutse-eetika koodeksi.

ISACA liikmed ja ISACA sertifikaatide omanikud peavad järgima alljärgnevat.

1. Toetama asjakohaste standardite, protseduuride ja meetmete rakendamist infosüsteemidele ning õhutama neile standarditele, protseduuridele ja meetmetele vastavuse saavutamist.

2. Täitma oma kohustusi vajaliku ja elukutselise hoolikusega, vastavalt kutseala standarditele ja parimatele tavadele.

3. Teenima seaduslikult ja ausalt huvirühmade huve, säilitades kõrgeid käitumis- ja iseloomunorme ning sattumata elukutset diskrediteerivatesse toimingutesse.

4. Hoidma oma ülesannete täitmise käigus saadud teabe privaatsust ja konfidentsiaalsust, kui selle teabe paljastamist ei nõua ametivõimud. Sellist teavet ei tohi kasutada isikliku kasu saamiseks ega avaldada ebakohastele pooltele.

5. Olema pidevalt oma erialadel pädev ja nõustuma ette võtma ainult selliseid tegevusi, mille puhul võib mõistlikult eeldada nende kutsealaselt pädevat sooritamist.

6. Teavitama asjakohaseid pooli sooritatud töö tulemustest, avaldades neile kõik teadaolevad olulised tõsiasjad.

7. Toetama huvirühmade erialast koolitust, nii et nad paremini tunneksid infosüsteemide turvet ja juhtimist.

Kutse-eetika koodeksi rikkumine võib viia liikme või sertifikaadiomaniku käitumise uurimiseni ja lõppkokkuvõttes distsiplinaarmeetmete rakendamiseni.

Kuidas kasutada seda väljaannet

Standardite seos suuniste ja protseduuridega

Infosüsteemide (IS) auditeerimise standardid on kohustuslikud nõuded sertifikatsiooniomanike aruannetele auditi ja selle leidude kohta. IS auditeerimise suunised ja protseduurid on detailsed juhised selle kohta, kuidas neid standardeid järgida. IS auditi suunised on juhised, mida IS audiitor harilikult järgib, kuid arusaadavalt võib ette tulla olukordi, kus audiitor neid juhiseid ei järgi. Sellisel juhul on IS audiitori kohus põhjendada töö sooritamise viisi. Protseduuride näited kirjeldavad IS audiitori sooritatavaid samme ja on informatiivsemad kui IS auditeerimise suunised. Näited on koostatud järgima IS auditeerimise standardeid ja IS auditeerimise suuniseid ning nad annavad teavet IS auditeerimise standardite järgimise kohta. Mõningal määral loovad nad järgitavate protseduuride jaoks ka parimad tavad.

Kodifitseerimine

Standardid on nummerdatud nende väljaandmisejärjestuses alates numbrist S1.

Suunised on nummerdatud nende väljaandmisejärjestuses alates numbrist G1.

Protseduurid on nummerdatud nende väljaandmisejärjestuses alates numbrist P1.

Kasutamine

IS audiitoril on soovitatav iga-aastase auditikava käigus ning ka aasta jooksul sooritatavate üksikläbivaatuste ajal vaataks läbi standardid, et veenduda neile vastavuses. IS audiitor võib aruandes viidata ISACA standarditele, öeldes, et läbivaatus sooritati vastavalt asukohamaa seadustele, kohaldatavatele auditi eeskirjadele ja ISACA standarditele.

Elektroonilised koopiad

Kõik ISACA standardid, suunised ja protseduurid on avaldatud ISACA veebisaidis aadressil *www.isaca.org/standards*.

Sõnastik

Täieliku terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary.*

Ülevaade infosüsteemide auditeerimise standarditest

ISACA väljaantud

Infosüsteemide auditeerimise spetsialiseeritud iseloom ja selliste auditite sooritamiseks vajalikud oskused nõuavad standardeid, mida rakendatakse spetsiifiliselt IS auditeerimisele. Üks ISACA® sihte on edendada ülemaailmselt rakendatavaid standardeid oma nägemuse saavutamiseks. IS auditeerimise standardite väljatöötamine ja levitamine on nurgakivi, millele on rajatud ISACA erialane panus audiitorkonna töösse. IS auditeerimise standardite raamstruktuur annab juhiseid mitmel tasemel.

- **Standardid** määratlevad kohustuslikke nõudeid IS auditeerimisele ja aruandlusele. Nad teavitavad
  - IS audiitoreid minimaalsest vastuvõetav soorituse tasemest, mis on nõutav IS audiitorite kutse-eetika ISACA koodeksis sõnastatud kutsealaste kohustuste täitmiseks;
  - juhtkondaja teisi huvipooli kutseala nõuetest, mis puudutavad sel ala tegutsejate tööd;
  - sertifitseeritud infosüsteemiaudiitori (CISA®) tiitli kandjaid nõuetest. Nende standardite rikkumise tulemuseks võib olla CISA käitumise uurimine ISACA juhatuses või asjakohases ISACA komitees ning lõppkokkuvõttes distsiplinaarmeetmete rakendamine.
- **Suunised** annavad juhiseid IS auditeerimise standardite rakendamise kohta. IS audiitor peaks neid arvestama standardite rakendusviisi otsustamisel, kasutama nende rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama kõiki lahknevusi. IS auditeerimise suuniste eesmärk on anda lisateavet selle kohta, kuidas saavutada vastavust IS auditeerimise standarditele.
- **Protseduurid** toovad näiteid nende protseduuride kohta, mida IS audiitoril tuleb võib-olla sooritada auditiülesande täitmisel. Protseduuridokumendid annavad teavet selle kohta, kuidas IS auditeerimise töö sooritamisel järgida standardeid, kuid ei esita nõudeid. IS auditeerimise protseduuride eesmärk on anda lisateavet selle kohta, kuidas saavutada vastavust IS auditeerimise standarditele.

Info- ja sidustehnoloogia juhtimiseesmärgid **(COBIT®)** on infotehnoloogia (IT) haldamise raamstruktuur ja abivahendite kogum, mis võimaldab juhtidel ületada lõhesid juhtimisnõuete, tehniliste küsimuste ja tegutsemisriskide vahel. COBIT võimaldab välja töötada selge poliitika ja hea tava IT juhtimiseks tervete organisatsioonide ulatuses. Ta rõhutab vastavust õigusaktidele, aitab organisatsioonidel suurendada IT-st saadavat väärtust, võimaldab ühtlustust ja lihtsustab COBITi raamstruktuuri evitamist. COBIT on mõeldud kasutamiseks talitlusalasele ja IT juhtkonnale ning IS audiitoritele, seetõttu võimaldab ta kasutamine mõista talitlusalaseid eesmärke, teha teatavaks parimad tavad ja anda soovitusi ühe üldarusaadava ja maineka raamstruktuuri najal. COBIT on allalaadimiseks saadaval ISACA veebisaidis *www.isaca.org/cobit*. COBITi raamstruktuur määratleb, et kõiki alljärgnevaid temaga seotud tooteid ja/või elementeorganiseerib IT halduse protsess.

Ülevaade infosüsteemide auditeerimise standarditest (jätkub)

- Juhtimiseesmärgid – IT-protsesside suhtes minimaalse hea juhtimise üldistatud sõnastused.
- Juhtkonna suunised – juhised selle kohta, kuidas hinnata ja täiustada IT-protsesside sooritust küpsusmudelite, RACI-rollitabelite (RACI = omanik - kinnitaja - nõuandja - informeeritav), sihtide ja mõõdustiku abil. Nad loovad juhtkonnale orienteeritud raamstruktuuri pideva ja ettenägeliku juhtimise enesehindamisele, mille keskmes on eriti järgmised aspektid:
  - soorituse mõõtmine,
  - IT juhtimise profileerimine,
  - teadlikkus,
  - mõõtlemine.
- COBITi juhtimistavad – riski ja väärtuste määrangud ning juhtimiseesmärkide evitamise juhised.
- IT tagamise juhend – juhised selle kohta, kuidas igas juhtimislõigus omandada arusaamist, hinnata iga meedet, hinnata vastavust ja konkretiseerida meetmete rakendamata jätmisest tulenevat riski.

Terminite sõnastiku võib leida ISACA veebisaidist, aadressilt *www.isaca.org/glossary*. Sõnu "audit" ja "läbivaatus" kasutatakse ISACA standardites, suunistes ja protseduurides ühesuguses tähenduses.

Lahtiütlus. ISACA on kavandanud need juhised vastuvõetava sooritusе minimaalse tasemena, mis on vajalik ISACA infosüsteemiaudiitorite kutse-eetika koodeksis sõnastatud kutsealaste kohustuste täitmiseks. ISACA ei väida, et selle toote kasutamine tagab eduka tulemuse. Seda väljaannet ei tohiks vaadelda sellisena, mis sisaldaks mingeid õigeid protseduure ja teste või välistaks muid protseduure ja teste, mis on mõistlikult suunatud samade tulemuste saamisele. Iga konkreetse protseduuri või testi õigsuse määramisel peaks meetmete spetsialist rakendama oma kutsealast otsustusoskust konkreetsetele juhtimisolukordadele, mis tulevad ette konkreetsetes süsteemides või infotehnoloogilistes keskkondades.

ISACA standardinõukogu on IS auditeerimise standardite, suuniste ja protseduuride koostamisel toetunud laialdasele konsulteerimisele. Enne mingi dokumendi väljaandmist avaldab standardinõukogu rahvusvahelises ulatuses tutvustuskavandeid kommentaaride saamiseks avalikkuselt. Vajadusel otsib standardinõukogu konsulteerimiseks ka inimesi, kes on käsitletava teema alal asjatundjad või kes on sellest teemast huvitatud. Standardinõukogul on pideva arenduse kava ning talle on tekkivate ja uusi standardeid nõudvate küsimuste väljaselgitamiseks teretulnud vastavad andmed ISACA liikmetelt ja muudelt huvirühmadelt. Kõik ettepanekud tuleks meilida (standards@isaca.org), faksida (+1.847. 253.1443) või saata postiga ISACA rahvusvahelisele peakontorile aadressil ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008 USA, kus neid käsitleb uurimisstandardite ja akadeemiliste sidemete ala juhataja.

Jõustumiskuupäev

Infosüsteemide auditeerimise standardite register

S1 Audititalituse põhikiri	1. jaanuar	2005
S2 Sõltumatus	1. jaanuar	2005
S3 Kutse-eetika ja standardid	1. jaanuar	2005
S4 Kutsealane pädevus	1. jaanuar	2005
S5 Plaanimine	1. jaanuar	2005
S6 Audititöö sooritamine	1. jaanuar	2005
S7 Aruandlus	1. jaanuar	2005
S8 Järeltoimingud	1. jaanuar	2005
S9 Korratused ja ebaseaduslikud toimingud	1. september	2005
S10 IT ohje	1. september	2005
S11 Riski kaalutlemise kasutamine auditi plaanimisel	1. november	2005
S12 Kaalukus auditis	1. juuli	2006
S13 Teiste asjatundjate töö kasutamine	1. juuli	2006
S14 Auditi asitõendid	1. juuli	2006
S15 IT juhtimismeetmed	1. veebruar	2008
S16 E-kaubandus	1. veebruar	2008

Infosüsteemide auditeerimise suuniste register

G1 Teiste audiitorite töö kasutamine	1. juuni 1998 uus versioon:	1. märts	2008
G2 Auditi asitõendite nõue	1. detsember 1998 uus versioon:	1. mai	2008
G3 Arvutipõhiste auditimeetodite (CAAT) kasutamine	1. detsember 1998 uus versioon:	1. märts	2008
G4 IS-tegevuste tellimine teistelt organisatsioonidelt	1. september 1999 uus versioon:	1. mai	2008
G5 Audititalituse põhikiri	1. september 1999 uus versioon:	1. veebruar	2008
G6 Kaalukuse kontseptsioonid infosüsteemide auditeerimisel	1. september 1999 uus versioon:	1. mai	2008
G7 Kutsealane hoolikus	1. september 1999 uus versioon:	1. märts	2008
G8 Auditi dokumentatsioon	1. september 1999 uus versioon:	1. märts	2008
G9 Korratuste arvestamine auditeerimisel		1. märts	2000
G10 Valimkontroll auditeerimisel		1. märts	2000
G11 IS üldmeetmete toime		1. märts	2000
G12 Organisatsiooniline seos ja sõltumatus		1. september	2000
G13 Riski kaalutlemise kasutamine auditi plaanimisel		1. september	2000
G14 Rakendussüsteemide läbivaatus		1. november	2001
G15 Plaanimine		1. märts	2002

Jõustumiskuupäev

Infosüsteemide auditeerimise suuniste register (jätkub)

G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele	1. märts	2002
G17 Auditivälise rolli mõju IS audiitori sõltumatusele	1. juuli	2002
G18 IT haldus	1. juuli	2002
G19 Korratused ja ebaseaduslikud toimingud	1. juuli	2002
G20 Aruandlus	1. jaanuar	2003
G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus	1. august	2003
G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus	1. august	2003
G23 Süsteemi arengu elutsükli (SAE) läbivaatused	1. august	2003
G24 Interneti-pangandus	1. august	2003
G25 Virtuaalsete privaatvõrkude läbivaatus	1. juuli	2004
G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus	1. juuli	2004
G27 Mobiilne andmetöötlus	1. september	2004
G28 Arvutikriminalistika	1. september	2004
G29 Evitusjärgne läbivaatus	1. jaanuar	2005
G30 Pädevus	1. juuni	2005
G31 Privaatsus	1. juuni	2005
G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt	1. september	2005
G33 Interneti kasutamise üldised kaalutlused	1. märts	2006
G34 Kohustused, õigused ja vastutus	1. märts	2006
G35 Järeltoimingud	1. märts	2006
G36 Biomeetrilised meetmed	1. veebruar	2007
G37 Konfiguratsioonihalduse protsess	1. november	2007
G38 Pääsu reguleerimise meetmed	1. veebruar	2008
G39 IT korraldus	1. mai	2008

Infosüsteemide auditeerimise protseduuride register

P1 IS riski kaalutlemine	1. juuli	2002
P2 Digitaalallkirjad	1. juuli	2002
P3 Sissetungi avastamine	1. august	2003
P4 Viirused ja muu kahjurkood	1. august	2003

Jõustumiskuupäev

Infosüsteemide auditeerimise protseduuride register (jätkub)

P5 Juhtimisriski isehindamine	1. august	2003
P6 Tulemüürid	1. august	2003
P7 Korratused ja ebaseaduslikud toimingud	1. november	2003
P8 Turvalisuse hindamine. Läbistustestimine ja nõrkuste analüüs	1. september	2004
P9 Krüpteerimismetoodikate halduse meetmete hindamine	1. jaanuar	2005
P10 Ärirakenduse muutmise ohje	1. oktoober	2006
P11 Elektrooniline arveldus (EFT)	1. mai	2007

Infosüsteemide auditeerimise standardid

ISACA väljaantud

S1 Audititalituse põhikiri

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle IS auditeerimise standardi eesmärk on kehtestada audititalituse põhikiri, mida kasutatakse auditeerimisprotsessi kestel, ja anda selle kohta juhiseid.

Standard

03 Infosüsteemide auditi talituse või infosüsteemide auditi ülesande täitja eesmärk, kohustused, õigused ja vastutus peaksid olema auditi põhikirjas või töövõtukirjas selgelt dokumenteeritud.

04 Auditi põhikiri või töövõtukiri tuleks organisatsiooni(de) asjakohasel tasemel kokku leppida ja kinnitada.

Kommentaarid

05 Sisemise infosüsteemide auditi talituse sooritatavate tegevuste kohta tuleks koostada põhikiri. Kui kohustused varieeruvad või muutuvad, tuleks audititalituse põhikiri vähemalt kord aastas läbi vaadata. Sisemine IS audiitor saab töövõtukirjas täpsemalt selgitada või kinnitada osalust konkreetsetes auditeerimis- või muudes ülesannetes. Välise infosüsteemide auditi puhul tuleks tavaliselt koostada töövõtukiri iga auditeerimis- või muu ülesande puhuks.

06 Audititalituse põhikiri või töövõtukiri peaks olema audititalituse või auditiülesande eesmärgi, kohustuste ja kitsenduste väljendamiseks piisavalt detailne.

07 Audititalituse põhikiri või töövõtukiri tuleks perioodiliselt läbi vaadata, veendumiseks, et eesmärk ja kohustused on dokumenteeritud.

08 Auditi põhikirja või tellimiskirja koostamise kohta annavad lisateavet järgmised juhised:

- IS auditeerimise suunis G5 "Audititalituse põhikiri",
- COBITi raamstruktuur, juhtimiseesmärk SH4.

Jõustumiskuupäev

09 See ISACA standard kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. jaanuaril 2005 või pärast seda.

S2 Sõltumatus

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle IS auditeerimise standardi eesmärk on kehtestada standardid sõltumatuse kohta auditeerimisprotsessi kestel, ja anda selle kohta juhiseid.

Standard

03 Kutsealane sõltumatus

Kõigis auditiga seotud küsimustes peaks IS audiitor olema auditeeritavast sõltumatu nii oma hoiakult kui ka esinemiselt.

04 Organisatsiooniline sõltumatus

IS auditi talitus peaks auditiülesande objektiivseks sooritamiseks olema sõltumatu läbivaadatavast tegevusvaldkonnast.

Kommentaarid

05 Audititalituse põhikiri või töövõtukiri peaks käsitlema audititalituse sõltumatust ja vastutust.

06 IS audiitor peaks alati olema ja tunduma sõltumatu nii oma hoiakult kui ka esinemiselt.

07 Kui sõltumatust on tegelikult või näiliselt rikutud, tuleks rikkumise üksikasjad avaldada asjakohastele pooltele.

08 IS audiitor peaks olema organisatsiooniliselt sõltumatu auditeeritavast tegevusvaldkonnast.

09 Sõltumatust peaksid regulaarselt hindama IS audiitor, juhtkond ja auditikomisjon, kui see on olemas.

10 Mingis IS-ürituses loomult auditivälises rollis osalev IS audiitorei pea olema ega näima sõltumatu, kui seda ei nõua muud kutseala standardid ega reguleerivad organid.

11 Kutsealase või organisatsioonilise sõltumatuse kohta annavad lisateavet järgmised juhised:

- IS auditeerimise suunis G17 "Auditivälise rolli mõju IS audiitori sõltumatusele";
- IS auditeerimise suunis G12 "Organisatsiooniline seos ja sõltumatus";
- COBITi raamstruktuur, juhtimiseesmärk SH4.

Jõustumiskuupäev

12 See ISACA standard kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. jaanuaril 2005 või pärast seda.

S3 Kutse-eetika ja standardid

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle IS auditeerimise standardi eesmärk on kehtestada IS audiitorile standard ISACA kutse-eetika koodeksi järgimise ja kutsealase hoolikuse kohta auditiülesannete täitmisel ning anda talle selle kohta juhiseid.

Standard

05 IS audiitor peaks auditiülesannete täitmisel järgima ISACA kutse-eetika koodeksit.

06 Auditiülesannete täitmisel peaks IS audiitor ilmutama vajalikku kutsealast hoolikust, sealhulgas järgima kohaldatavaid kutsealaseid auditeerimise standardeid.

Kommentaarid

07 ISACA väljaantud kutse-eetika koodeksit muudetakse aeg-ajalt, et pidada sammu auditeerimiskutse alal tekkivate tendentside ja nõuetega. ISACA liikmed ja IS audiitorid peaksid joonduma uusima kutse-eetika koodeksi järgi ning järgima seda oma kohustuste täitmisel IS audiitoritena.

08 ISACA väljaantud IS auditeerimise standardeid vaadatakse nende pidevaks täiustamiseks perioodiliselt läbi ja vajadusel muudetakse neid, et pidada sammu auditeerimiskutse alal tekkivate uute ülesannetega. ISACA liikmed ja IS audiitorid peaksid olema teadlikud uusimatest kohaldatavaist IS auditeerimise standarditest ja ilmutama auditiülesannete täitmisel kutsealast hoolikust.

09 ISACA kutse-eetika koodeksi ja või IS auditeerimise standardite rikkumine võib viia liikme või sertifikaadiomaniku käitumise uurimiseni ja lõppkokkuvõttes distsiplinaarmeetmete rakendamiseni.

10 ISACA liikmed ja IS audiitorid peaksid vahetama teavet oma töörühma liikmetega ning tagama, et töörühmad auditiülesannete täitmisel peavad kinni kutse-eetika koodeksist ja jälgivad kohaldatavaid IS auditeerimise standardeid.

11 Auditiülesande täitmisel peaksid IS audiitorid asjakohaselt käsitlema kõiki kutse-eetika või IS auditeerimisee standardite rakendamisel ilmnenud probleeme. Kui kutse-eetika või IS auditeerimisee standardite järgimisega on või näib olevat raskusi, peaks IS audiitor kaaluma ülesande täitmisest loobumist.

12 IS audiitor peaks säilitama võimalikult väärika moraalse hoiaku ja käitumise ega kasutama auditiülesannete saamiseks või täitmiseks meetodeid, mis võivad tunduda ebaseaduslikud, ebaeetilised või ebaprofessionaalsed.

S3 Kutse-eetika ja standardid (jätkub)

11 Lisateabe saamiseks kutse-eetika ja standardite kohta tuleks toetuda järgmistele juhistele:

- IS auditeerimise suunis G19 "Korratused ja ebaseaduslikud toimingud";
- IS auditeerimise suunis G7 "Kutsealane hoolikus";
- IS auditeerimise suunis G12 "Organisatsiooniline seos ja sõltumatus";
- COBITi raamstruktuur, juhtimiseesmärk SH4.

Jõustumiskuupäev

12 See IS auditeerimise standard kehtib kõigi infosüsteemiauditite kohta alates 1. jaanuarist 2005.

S4 Kutsealane pädevus

Sissejuhatus

01 ISACA IS auditeerimise standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle IS auditeerimise standardi eesmärk on kehtestada nõuded ja anda juhiseid selle kohta, kuidas IS audiitor saavutab ja säilitab kutsealase pädevuse.

Standard

03 IS audiitor peaks olema kutsealaselt pädev, tal peaksid olema auditiülesande täitmiseks vajalikud oskused ja teadmised.

04 IS audiitor peaks asjakohase pideva kutsealase õppe ja koolitusega hoidma ülal oma kutsealast pädevust.

Kommentaarid

05 Enne töö sooritamist peaks IS audiitor andma mõistliku kinnituse piisava kutsealase pädevuse (kavasoleva ülesandega seotud oskuste, teadmiste ja kogemuste) olemasolu kohta. Vastasel juhul peaks IS audiitor loobuma ülesande täitmisest.

06 Kui IS audiitoril on CISA või muu kutsealane auditiga seotud kvalifikatsioon, peaks ta täitma neist tulenevaid pideva kutsealase õppe või arengu nõudeid. Infosüsteemide auditeerimises osalevail ISACA liikmeil, kel ei ole CISA ega muud kutsealast auditiga seotud kvalifikatsiooni, peaks olema piisav formaalne haridus, koolitus ja töökogemus.

07 Kui IS audiitor juhib rühma mingi läbivaatuse sooritamiseks, peab ta andma mõistliku kinnituse selle kohta, et kõigil rühma liikmetel on oma töö sooritamiseks asjakohane kutsealase pädevuse tase.

08 Lisateabe saamiseks kutsealase pädevuse kohta tuleks toetuda järgmistele juhistele:

- CISA sertifitseerimis- ja koolitusmaterjal;
- CISA pideva sertifitseerimise ja õppe nõuded;
- COBITi raamstruktuur, juhtimiseesmärgid SH2, SH3 ja SH4.

Jõustumiskuupäev

09 See IS auditeerimise standard kehtib kõigi infosüsteemiauditite kohta alates 1. jaanuarist 2005.

S5 Plaanimine

Sissejuhatus

01 ISACA IS auditeerimise standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle IS auditeerimise standardi eesmärk on kehtestada nõuded ja anda juhiseid auditi plaanimise kohta.

Standard

03 IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele.

04 IS audiitor peaks välja töötama ja dokumenteerima riskipõhise auditeerimismetoodika.

05 IS audiitor peaks välja töötama ja dokumenteerima auditi plaani, mis loetleks auditi ajastuse ja ulatuse, eesmärgid ja vajalikud ressursid, detailiseerides auditi iseloomu ja eesmärgid.

06 IS audiitor peaks välja töötama auditi kava ja/või plaani, mis detailiseeriks auditi sooritamiseks vajalike protseduuride iseloomu, ajastuse ja ulatuse.

Kommentaarid

07 Sisemise audititalituse jaoks tuleks vähemalt kord aastas koostada või ajakohastada käsilolevate tegevuste plaan. See plaan peaks moodustama audititegevuste raamstruktuuri ja hõlmama auditi põhikirjas määratud kohustusi. Uue või ajakohastatud plaani peaks kinnitama auditikomisjon, kui see on olemas.

08 Välise IS auditi puhul tuleks plaan tavaliselt koostada iga auditi- või muu ülesande kohta. See plaan peaks dokumenteerima auditi eesmärgid.

09 IS audiitor peab auditeeritava tegevuse endale selgeks tegema. Vajalike teadmiste ulatus tuleks määrata organisatsiooni iseloomu ja keskkonna, riskide ja auditi eesmärkide järgi.

10 Mõistliku kinnituse saamiseks sellele, et auditi ajal hõlmatakse adekvaatselt kõik kaalukad asjad, peaks IS audiitor sooritama riski kaalutlemise. Seejärel saab välja töötada auditi strateegiad, kaalukuse tasemed ja ressursid.

11 Auditi ajal ilmnevate asjaolude (uued riskid, väärad eeldused või juba sooritatud protseduuridega saadud leiud) käsitlemiseks tuleb auditi kava ja/või plaani võib-olla korrigeerida auditi käigus.

12 Lisateabe saamiseks auditi põhikirja või töövõtukirja koostamise kohta tuleks toetuda järgmistele juhistele:

- IS auditeerimise suunis G6 "Kaalukuse kontseptsioonid infosüsteemide auditeerimisel";
- IS auditeerimise suunis G15 "Plaanimine";

S5 Plaanimine (jätkub)

- IS auditeerimise suunis G13 "Riski kaalutlemise kasutamine auditi plaanimisel";
- IS auditeerimise suunis G16 "Kolmandate poolte mõju organisatsiooni IT-meetmetele";
- COBITi raamstruktuur, juhtimiseesmärgid.

Jõustumiskuupäev

13 See IS auditeerimise standard kehtib kõigi infosüsteemiauditite kohta alates 1. jaanuarist 2005.

S6 Audititöö sooritamine

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle IS auditeerimise standardi eesmärk on kehtestada nõuded ja anda juhiseid audititöö sooritamise kohta.

Standard

03 Järelevalve. IS auditi personalile tuleks rakendada järelevalve mõistliku kinnituse saamiseks sellele, et auditi eesmärgid saavutatakse ja kohaldatavaid kutsealaseid auditeerimisstandardeid järgitakse.

04 Asitõendid. Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega.

05 Dokumenteerimine. Auditiprotsess tuleks dokumenteerida, kirjeldades sooritatud auditööd ja auditi asitõendeid, mis toetavad IS audiitori leide ja järeldusi.

Kommentaarid

06 Auditi alustamisel tuleks kehtestada IS auditi töörühma rollid ja kohustused, määratledes vähemalt otsustajate, täitjate- ja läbivaatajate rollid.

07 Ülesande täitmise ajal sooritatav töö tuleks korraldada ja dokumenteerida järgides ettemääratud dokumenteeritud protseduure. Dokumentatsioon peaks sisaldama töö eesmärke ja käsitlusala, auditi kava, sooritatud auditisamme, kogutud asitõendeid, leide, järeldusi ja soovitusi.

08 Auditi dokumentatsioon peaks olema piisav selleks, et mingi sõltumatu pool saaks samadele järeldustele jõudmiseks uuesti sooritada kõik auditi käigus sooritatud tööd.

09 Auditi dokumentatsioon peaks sisaldama iga audititöökohta üksikasju, mis näitavad, kes selle töö sooritasid ja millised olid nende rollid. Üldreeglina peaks iga töö, otsuse, sammu või auditi tulemi, mille tegi töörühma liige või liikmete grupp, läbi vaatama selle töörühma teine liige, kes määratakse käsitletu tähtsusele vastavalt.

10 IS audiitor peaks plaanima kasutada parimaid auditi asitõendeid, mida on võimalik saada vastavalt auditi eesmärgi tähtsusele ning nende asitõendite saamiseks vajalikule aja- ja töökulule.

11 Auditi asitõendid peavad olema arvamuse kujundamiseks või IS audiitori leidude ja järelduste toetamiseks piisavad, usaldusväärsed ning asjassepuutuvad ja kasulikud. Kui saadud auditi asitõendid ei vasta IS audiitori arvates neile kriteeriumidele, peaks IS audiitor hankima täiendavaid auditi asitõendeid.

S6 Audititöö sooritamine (jätkub)

12 Lisateabe saamiseks audititöö sooritamise kohta tuleks toetuda järgmistele juhistele:

- COBITi raamstruktuur, juhtimiseesmärgid.

Jõustumiskuupäev

13 See IS auditeerimise standard kehtib kõigi infosüsteemiauditite kohta alates 1. jaanuarist 2005.

S7 Aruandlus

Sissejuhatus

01 ISACA IS auditeerimise standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle IS auditeerimise standardi eesmärk on kehtestada nõuded ja anda juhiseid aruandluse kohta, nii et IS audiitor saaks seda kohustust täita.

Standard

03 Pärast auditi lõpuleviimist peaks IS audiitor koostama sobivas vormis aruande. Aruandesse tuleks märkida organisatsioon, eeldatavad saajad ja võimalikud levituskitsendused.

04 Auditi aruanne peaks teatama sooritatud audititöö käsitlusala, eesmärgid, hõlmatud perioodi, ajastuse ja ulatuse.

05 Aruanne peaks teatama leiud, järeldused ja soovitused ning kahtlused, piirangud või käsitlusala kitsendused, mis IS audiitoril võivad olla auditi suhtes.

06 IS audiitoril peaksid aruandes esitatud tulemuste toetuseks olema piisavad ja asjakohased auditi asitõendid.

07 Väljastamisel tuleks IS audiitori aruanne varustada allkirja ja kuupäevaga ning levitada vastavalt auditi põhikirja või töövõtukirja tingimustele.

Kommentaarid

08 Aruande vorm ja sisu varieerub harilikult teenuse või ülesande tüübi mõttes. IS audiitor võib sooritada töid järgmiste hulgast:

- audit (otsene või tõenduse audit),
- läbivaatus (otsene või tõenduse audit),
- kokkulepitud protseduurid.

09 Kui IS audiitoril tuleb ülesande raames esitada arvamus juhtimiskeskkonna kohta ning tal on auditi asitõendeid kaaluka või olulise nõrkuse kohta, peaks ta välistama järelduse, et sisemised meetmed on toimivad. IS audiitori aruanne peaks kirjeldama kaalukat või olulist nõrkust ning selle toimet juhtimiskriteeriumide eesmärkide saavutamisele.

10 IS audiitor peaks aruandekavandi sisu enne lõplikku vormistamist ja väljastamist läbi arutama käsitletava ala juhtkonnaga ning lisama lõplikku aruandesse asjassepuutuvad juhtkonna kommentaarid.

11 Kui IS audiitor leiab juhtimiskeskkonnas olulisi nõrkusi, peaks ta neist teatama auditikomisjonile või vastutavale organile ning märkima aruandesse, et olulistest nõrkustest on teatatud.

12 Kui IS audiitor väljastab eraldi aruanded, peaks lõplik aruanne viitama kõigile eraldi aruannetele.

S7 Aruandlus (jätkub)

13 IS audiitor peaks kaaluma ja otsustama, kas teatada juhtkonnale sellistest sisejuhtimise puudustest, mis on olulistest puudustest väiksemad. Sellistel juhtudel peaks IS audiitor teatama auditikomisjonile või vastutavale organile, et niisugustest sisejuhtimise puudustest on juhtkonnale teatatud.

14 IS audiitor peaks küsima asjakohast teavet eelmise aruande leidude, järelduste ja soovituste kohta, ning hindama seda otsustamiseks, kas õigel ajal rakendati asjakohaseid meetmeid.

15 Lisateabe saamiseks aruandluse kohta tuleks toetuda järgmistele juhistele:

- IS auditeerimise suunis G20 "Aruandlus";
- COBITi raamstruktuur, juhtimiseesmärgid SH4.7 ja SH4.8

Jõustumiskuupäev

16 See IS auditeerimise standard kehtib kõigi infosüsteemiauditite kohta alates 1. jaanuarist 2005.

S8 Järeltoimingud

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle IS auditeerimise standardi eesmärk on kehtestada nõuded ja anda juhiseid IS auditi protsessi käigus sooritatavate järeltoimingute kohta.

Standard

03 Pärast leidude ja soovituste teatamist aruandes peaks IS audiitor taotlema asjakohast teavet ja hindama seda otsustamiseks, kas juhtkond on õigel ajal rakendanud asjakohaseid meetmeid.

Kommentaarid

04 Kui IS audiitoriga on arutatud juhtkonna pakutud meetmeid aruandes olevate soovituste elluviimiseks või talle on need teatatud, tuleks need meetmed juhtkonna reaktsioonina märkida lõpparuandesse.

05 Järeltoimingute iseloom, ajastus ja ulatus peaks arvestama aruandes teatatud leidude olulisust ja nende toimet parandusmeetmete rakendamata jätmise korral. IS auditi algsest aruandlusest tulenevate järeltoimingute ajastus peaks olema kutsealase otsustuse küsimus ning sõltuma mitmetest kaalutlustest, näiteks üksuse jaoks kaasnevate riskide ja kulude iseloomust või suurusest.

06 Sisemine IS auditi talitus peaks rajama protsessi, millega seirata ja tagada, et juhtkonna meetmed on toimivalt rakendatud või et kõrgem juhtkond on aktsepteerinud meetmete rakendamata jätmisest tuleneva riski. Kohustused niisuguste järeltegevuste osas võib määratleda talituse auditi põhikirjas.

07 Sõltuvalt oma ülesande käsitlusalast ja tingimustest võivad välised IS audiitorid toetuda oma kokkulepitud soovituste järeltoimingute osas sisemisele IS auditi talitusele.

08 Kui juhtkond annab teavet soovituste elluviimiseks rakendatud meetmete kohta, kuid IS audiitoril on selle teabe suhtes kahtlusi, tuleks enne järeltoimingute lõpuleviimist läbi viia asjakohane testimine või muud protseduurid asjade tegelikus seisus veendumiseks.

09 Auditikomisjonile (kui see on olemas) või üksuse juhtkonna asjakohasele tasemele võidakse esitada järeltoimingute seisu kohta aruanne, milles on märgitud kokkulepitud, kuid rakendamata jäänud soovitused.

10 Järeltoimingute ühe osana peaks IS audiitor hindama, kas leiud on meetmete rakendamata jätmisel jäänud püsima.

Jõustumiskuupäev

16 See IS auditeerimise standard kehtib kõigi infosüsteemiauditite kohta alates 1. jaanuarist 2005.

S9 Korratused ja ebaseaduslikud toimingud

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle ISACA standardi eesmärk on kehtestada nõuded ja anda juhiseid korratuste ja ebaseaduslike toimingute kohta, mida IS audiitor peaks auditiprotsessi käigus arvestama.

Standard

03 Auditi plaanimisel ja sooritamisel peaks IS audiitor riski piisavaks vähendamiseks arvestama korratuste ja ebaseaduslike toimingute riski.

04 Auditi ajal peaks IS audiitor säilitama kutsealase skeptilise hoiaku ning arvestama, et kuigi ta on hinnanud korratuste ja ebaseaduslike toimingute riski, võivad korratuste ja ebaseaduslike toimingute tõttu esineda kaalukad väärad olukorra esitused.

05 IS audiitor peaks organisatsiooni, selle keskkonna ja sisemeetmed endale selgeks tegema.

06 IS audiitor peaks hankima piisavaid ja asjakohaseid auditi asitõendeid otsustamiseks, kas juhtkond või muud organisatsiooni kuulujad teavad mingeid tegelikke, kahtlustatavaid või oletatavaid korratusi või ebaseaduslikke toiminguid.

07 Auditiprotseduuride sooritamisel organisatsiooni ja ta keskkonna tundmaõppimiseks peaks IS audiitor pöörama tähelepanu ebatavalistele või ootamatutele seostele, mis võivad viidata korratustest ja ebaseaduslikest toimingutest tulenevatele kaalukatele vääresitustele.

08 IS audiitor peaks kavandama ja sooritama protseduure, millega testida sisejuhtimise sobivust ja juhtkonnapoolse meetmetest möödumise riski.

09 Kui IS audiitor tuvastab väärväite, peaks ta kaaluma, kas selline väärväide võib viidata mingile korratusele või ebaseaduslikule toimingule. Kui see on nii, peaks IS audiitor mõtlema, millised on selle tagajärjed auditi muudele aspektidele, eriti aga juhtkonna esitatud ettekannetele.

10 IS audiitor peaks sõltuvalt auditiülesandest vähemalt korra aastas või sagedamini saama juhtkonnalt kirjaliku ettekande. Ettekanne peaks

- **tunnistama juhtkonna kohustust kavandada ja rakendada sisemeetmeid korratuste ja ebaseaduslike toimingute välistamiseks;**
- **avaldama IS audiitorile korratusest või ebaseaduslikust toimingust tuleneva kaaluka väära teabeesituse riski kaalutlemise tulemused;**

S9 Korratused ja ebaseaduslikud toimingud (jätkub)

- **avaldama IS audiitorile korratused või ebaseaduslikud toimingud, mis on teada ja mõjutavad organisatsiooni ning on seotud**

  – juhtkonnaga,

  – töötajatega, kellel on sisejuhtimises olulised rollid;

- **avaldama IS audiitorile kõik teadaolevad töötajate, endiste töötajate, järelevalveametnike jt väited organisatsiooni mõjutavate tegelike või oletatavate korratuste või ebaseaduslike toimingute kohta.**

11 Kui IS audiitor tuvastab kaaluka korratuse või ebaseadusliku toimingu või saab teavet kaaluka korratuse või ebaseadusliku toimingu võimaliku asetleidmise kohta, peaks ta selle aegsasti teatavaks tegema asjakohasele juhtkonna tasemele.

12 Kui IS audiitor tuvastab kaaluka korratuse või ebaseadusliku toimingu, millesse on segatud juhtkond või töötajad, kellel on oluline roll sisejuhtimises, peaks ta selle aegsasti teatavaks tegema kõrgema võimu kandjaile.

13 IS audiitor peaks nõustama asjakohast juhtkonna taset ja kõrgema võimu kandjaid sisejuhtimise meetmete kavanduse ja teostuse kaalukate nõrkuste küsimuses, nii et väditaks ja avastataks korratused ja ebaseaduslikud toimingud, mis võisid IS audiitorile ilmneda auditi käigus.

14 Kui IS audiitor sattub erandlikku olukorda, mis kaaluka väärväite või ebaseadusliku toimingu tõttu mõjutab ta võimet jätkata auditi sooritamist, peaks ta kaaluma sellele olukorrale kohaldatavaid õiguslikke ja kutsealaseid kohustusi, sealhulgas seda, kas IS audiitor on kohustatud teatama ülesandes osalejaile või mõnedel juhtudel kõrgema võimu kandjaile või reguleerivale asutusele või kaaluma ülesande täitmisest loobumist.

15 IS audiitor peaks dokumenteerima kõik teabevahetused, plaanimised, tulemused, hindamised ja järeldused, mis puudutavad korratusi ja ebaseaduslikke toiminguid, millest on teatatud juhtkonnale, kõrgema võimu kandjaile, reguleerivatele asutustele ja teistele.

Kommentaarid

16 Korratuse ja ebaseadusliku toimingu määratlemiseks peaks IS audiitor toetuma IS auditeerimise suunisele G19 "Korratused ja ebaseaduslikud toimingud".

17 IS audiitor peaks hankima mõistliku kinnituse sellele, et korratuste ja ebaseaduslike toimingute tõttu ei ole kaalukaid väärväiteid. Otsustuste rakendamise, testimise ulatuse, sisemeetmete olemuslike piirangute jms tõttu ei või IS audiitor saada absoluutset kinnitust. Auditi ajal IS audiitori käsutuses olevad auditi asitõendid peaksid olema loomult pigem veenvad kui lõplikult otsustavad.

18 Ebaseaduslikust toimingust tuleneva kaaluka väärväite avastamata jäämise risk on suurem kui korratusest või veast tuleneva kaaluka väärväite avastamata jäämise risk, sest ebaseaduslikud toimingud sisaldavad keerukaid skeeeme, mis on kavandatud varjama IS audiitori eest sündmusi või sihilikke vääresitusi.

S9 Korratused ja ebaseaduslikud toimingud (jätkub)

19 Auditi ajal peaksid IS audiitorit abistama ta varasem kogemus ja organisatsiooni tundmine. Küsitluste korraldamisel ja auditiprotseduuride sooritamisel ei tarvitse IS audiitor täielikult kõrvale jätta senist kogemust, vaid peaks teataval määral säilitama kutsealase skeptitsismi. IS audiitor ei tohiks rahulduda väheveenvate auditi asitõenditega, mis põhinevad usul, et juhtkond ja kõrgema võimu kandjad on ausad ja korralikud. IS audiitor ja ülesande töörühm peaksid plaanimisprotsessi ühe osana ja kogu auditi kestel arutama organisatsiooni aldidust korratustele ja ebaseaduslikele toimingutele.

20 Kaalukate korratuste ja ebaseaduslike toimingute olemasolu riski hindamiseks peaks IS audiitor mõtlema sellele, kuidas kasutada ära

- oma varasemad teadmised ja kogemused selle organisatsiooni alal (sealhulgas oma kogemused juhtkonna ja kõrgema võimu kandjate aususe ja korralikkuse osas);
- juhtkonna küsitlemistega hangitud teave;
- juhtkonna ettekanded ja sisejuhtimise otsused;
- muu usaldusväärne auditi käigus hangitud teave;
- korratuste ja ebaseaduslike toimingute riski juhtkonnapoolne kaalutlemine ja ta protsess nende riskide tuvastuseks ja neile reageerimiseks.

21 Lisateabe saamiseks korratuste ja ebaseaduslike toimingute kohta tuleks toetuda järgmistele juhistele:

- IS auditeerimise suunis G5 "Audititalituse põhikiri";
- COBITi raamstruktuur, juhtimiseesmärgid TT3, TT5, TT9, TT11 ja PO6;
- Sarbanes-Oxley seadus aastast 2002;
- Välismaise korruptiivsuse seadus aastast1977.

Jõustumiskuupäev

16 See IS auditeerimise standard kehtib kõigi infosüsteemiauditite kohta alates 1. septembrist 2005.

S10 IT ohje

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle ISACA standardi eesmärk on kehtestada nõuded ja anda juhiseid IT ohje alade kohta, mida IS audiitor peaks auditiprotsessi käigus arvestama.

Standard

03 IS audiitor peaks IS talituse läbi vaatama ja otsustama, kas see talitus on kooskõlas organisatsiooni missiooni, visiooni, väärtuste, eesmärkide ja strateegiatega.

04 IS audiitor peaks kontrollima, kas IS talitusel on selge määrang sooritusе (toimivuse ja tõhususe) kohta, mida ootab organisatsiooni talitlus, ja hindama ta tulemusi.

05 IS audiitor peaks läbi vaatama IS ressursi- ja sooritusehalduse protsessid ja neid hindama.

06 IS audiitor peaks kontrollima ja hindama vastavust õiguslikele, keskkonna ja teabe kvaliteedi alastele ning usaldatavus- ja turvanõuetele.

07 IS talituse hindamiseks peaks IS audiitor kasutama mingit riskipõhist metoodikat.

08 IS audiitor peaks läbi vaatama organisatsiooni juhtimiskeskkonna ja seda hindama.

09 IS audiitor peaks läbi vaatama riskid, mis võivad kahjulikult mõjutada IS keskkonda, ja kaalutlema neid.

Lisajuhised

10 IS audiitor peaks toetuma IS auditeerimise suunisele G18 "IT haldus".

11 IS audiitor peaks läbi vaatama talitlusprotsesse toetava IS töökeskkonna riskid ja kaalutlema neid. IS auditeerimise tegevus peaks aitama organisatsioonil tuvastada ja hinnata olulisi riskile avatud kohti ning osalema riskihaldus- ja juhtimissüsteemide täiustamises.

12 IT halduse võib läbi vaadata eraldi või arvestada teda igal IS talituse läbivaatusel.

13 Lisateabe saamiseks IT halduse kohta tuleks IS audiitoril võtta tugipunktideks järgmised juhised:

- IS auditeerimise suunised

  - G5 "Audititalituse põhikiri";

  - G6 "Kaalukuse kontseptsioonid infosüsteemide auditeerimisel";

  - G12 "Organisatsiooniline seos ja sõltumatus";

S10 IT ohje (jätkub)

- G13 "Riski kaalutlemise kasutamine auditi plaanimisel";
- G15 "PLaanimine";
- G16 "Kolmandate poolte mõju organisatsiooni IT-meetmetele";
- G17 "Auditivälise rolli mõju IS audiitori sõltumatusele";

- COBITi juhtkonna suunised;
- COBITi raamstruktuur, juhtimiseesmärgid; see standard puudutab kõiki juhtimiseesmärke kõigil COBITi juhtimisaladel;
- Juhtkonna teavitamine IT halduse alal. 2. trükk. IT halduse instituut;
- IT juhtimiseesmärgid Sarbanes-Oxley seaduse osas. IT halduse instituut;
- Kohaldatavad võivad olla ka USA Sarbanes-Oxley seadus aastast 2002 ja muud spetsiifilised õigusaktid.

Jõustumiskuupäev

14 See ISACA standard kehtib kõigi infosüsteemiauditite kohta alates 1. septembrist 2005.

S11 Riski kaalutlemise kasutamine auditi plaanimisel

Sissejuhatus

01 ISACA IS auditeerimise standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle standardi eesmärk on kehtestada nõuded ja anda juhiseid riski kaalutlemise kasutamisele auditi plaanimisel.

Standard

03 Auditi üldplaani koostamisel ja prioriteetide määramisel IS auditi ressursside toimivaks jaotamiseks peaks IS audiitor kasutama sobivat riski kaalutlemise meetodit või metoodikat.

04 Üksikläbivaatuste plaanimisel peaks IS audiitor tuvastama ja kaalutlema riskid, mis puudutavad läbivadatavat ala.

Kommentaarid

05 Riski kaalutlemine on meetod, mida IS auditi vaatlusalas kasutatakse auditeeritavate üksuste uurimisel ja riskile kõige rohkem avatud alade valimisel IS aastaplaani võetavaks läbivaatuseks.

06 Auditeeritav üksus määratletakse iga organisatsiooni ja ta süsteemide mingi diskreetse lõiguna.

07 IS auditi vaatlusala tuleks määrata organisatsiooni IT strateegilise plaani ja tegutsemise tundmise ning vastutava juhtkonnaga arutamise põhjal.

08 Vähemalt kord aastas tuleks läbi viia ja dokumenteerida IS auditi plaani koostamist hõlbustavaid riski kaalutlemise üritusi. Organisatsiooni strateegilisi plaane, eesmärke ja ettevõtte riskihalduse raamstruktuuri tuleks käsitleda riski kaalutlemise ürituse ühe osana.

09 Auditiprojektide valimisel võimaldab riski kaalutlemine IS audiitoril kvantiteerida ja põhjendada IS auditeerimise plaani täitmiseks või konkreetse läbivaatuse sooritamiseks vajalike auditeerimisressursside mahtu. Riskitunnetuse põhjal saab IS audiitor ka seada plaanilistele läbivaatustele prioriteedid ja anda oma panuse riskihalduse raamstruktuuride dokumenteerimisse.

10 IS audiitor peaks sooritama ülevaadatava alaga seotud riskide eelkaalutlemise. Iga konkreetse läbivaatuse puhul peaksid IS auditi ülesande eesmärgid kajastama sellise riskikaalutluse tulemusi.

11 Pärast läbivaatuse lõpuleviimist peaks IS audiitor hoolitsema selle eest, et organisatsiooni ettevõtteriski halduse raamstruktuuri või riskiregistrit (kui see on välja töötatud) ajakohastataks, nii et ta kajastaks läbivaatuse ja sellele järgneva tegevuse leide ja soovitusi.

12 IS audiitor peaks toetuma IS auditeerimise suunisele G13 "Riski kaalutlemise kasutamine auditi plaanimisel" ja IS auditeerimise protseduurile P1 "IS riski kaalutlemise mõõtmine".

Jõustumiskuupäev

13 See standard kehtib kõigi infosüsteemiauditite kohta alates 1. novembrist 2005.

S12 Kaalukus auditis

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle IS auditeerimise standardi eesmärk on kehtestada nõuded ja anda juhiseid kaalukuse kontseptsiooni kohta auditis ning kaalukuse ja audi riski seose kohta.

Standard

03 Auditiprotseduuride iseloomu, ajastuse ja ulatuse määramisel peaks IS audiitor arvestama kaalukust auditis ja kaalukuse seost auditi riskiga.

04 Auditi plaanimisel peaks IS audiitor arvestama juhtimismeetmete võimalikku nõrkust või puudumist ja seda, kas niisugune juhtimise nõrkus või puudumine võiks tekitada infosüsteemis olulise puuduse või kaaluka nõrkuse.

05 IS audiitor peaks arvestama kumulatiivset toimet, mis võib väikesed juhtimise puudused ja nõrkused ning meetmete puudumise muundada oluliseks puuduseks või kaalukaks nõrkuseks infosüsteemis.

06 IS audiitori aruanne peaks näitama toimetuid meetmeid või meetmete puudumist ning meetmete puuduste olulisust ja nõrkuste võimalikkust, mis võivad viia olulise puuduseni või kaaluka nõrkuseni.

Lisajuhiseid

07 Auditi risk on risk, et IS audiitor jõuab auditi leidude põhjal väärale järeldusele. IS audiitor peaks ka olema teadlik auditi riski kolmest komponendist, nimelt olemuslikust riskist, juhtimisriskist ja avastamise riskist. Vt G13 "Riski kaalutlemise kasutamine auditi plaanimisel".

08 Auditi plaanimisel ja sooritamisel peaks IS audiitor püüdma vähendada auditi riski vastuvõetavalt väikeseks ja saavutada auditi eesmärke. See saavutatakse IS juhtimismeetmete ja nendega seotud meetmete asjakohase hindamisega.

09 Juhtimise nõrkus loetakse kaalukaks, kui juhtimise puudumise tulemusena ei õnnestu saada mõistlikku kinnitust sellele, et juhtimiseesmärk saavutatakse.

10 Kaalukaks liigitatud nõrkus tähendab, et

- meetmeid ei ole ja/või meetmeid ei rakendata ja/või meetmed ei toimi;
- ta põhjustab nõrkuste kasvu.

11 Kaalukas nõrkus on oluline puudus või oluliste puuduste kombinatsioon, mille tulemusena jäävad soovimatud sündmused vältimata või avastamata.

12 Kaalukuse ja IS audiitorile vastuvõetava auditi riski suuruse vahel on pöördseos, st mida suurem on kaalukus, seda väiksem on auditi riski vastuvõetavus, ja vastupidi. See võimaldab IS audiitoril määrata auditiprotseduuride iseloomu, ajastust ja ulatust. Kui näiteks IS audiitor konkreetse auditiprotseduuri plaanimisel otsustab, et kaalukus on väiksem, suurendab ta sellega auditi riski. Nüüd võib IS audiitor üritada seda

S12 Kaalukus auditis (jätkub)

kompenseerida kas meetmete testimise laiendamisega (juhtimisriski hinnangu vähendamiseks) või sisulise testimise protseduuride laiendamisega (avastamisriski hinnangu vähendamiseks).

13 Kui IS audiitoril on vaja otsustada, kas juhtimise puudus või juhtimise puuduste kombinatsioon on oluline puudus või kaalukas nõrkus, peaks ta hindama kompenseerivate meetmete mõju ja seda, kas sellised kompenseerivad meetmed toimivad.

14 Kaalukuse ja auditi riski hindamine võib IS audiitoril eri aegadel varieeruda sõltuvalt asjaoludest ja muutuvast keskkonnast.

15 IS audiitor peaks toetuma IS auditeerimise suunisele G6 "Olulisuse kontseptsioonid infosüsteemide auditeerimisel".

16 Lisateabe saamiseks kaalukuse kohta auditis tuleks toetuda järgmistele juhistele.

- IS auditeerimise suunised:

  - G2 "Auditi asitõendite nõue";

  - G5 "Audititalituse põhikiri";

  - G8 "Auditi dokumentatsioon";

  - G9 "Korratuste arvestamine auditeerimisel";

  - G13 "Riski kaalutlemise kasutamine auditi plaanimisel";

- COBIT 4.0. IT Halduse Instituut, 2005;
- IT juhtimiseesmärgid Sarbanes-Oxley seaduse osas. IT Halduse Instituut, 2004.

Jõustumiskuupäev

17 See ISACA standard kehtib kõigi infosüsteemiauditite kohta alates 1. juulist 2006.

S13 Teiste asjatundjate töö kasutamine

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle IS auditeerimise standardi eesmärk on kehtestada nõuded ja anda juhiseid IS audiitorile, kes kasutab auditis teiste asjatundjate tööd..

Standard

03 Asjakohastel juhtudel peaks IS audiitor mõtlema teiste asjatundjate töö kasutamisele auditis.

04 Enne ülesande käsilevõtmist peaks IS audiitor kaaluma teiste asjatundjate kutsealast kvalifikatsiooni, pädevust, asjassepuutuvat kogemust, ressursse, sõltumatust ja kvaliteedikujunduse protsesse, ning need peavad teda rahuldama.

05 IS audiitor peaks auditi ühe osana kaaluma, läbi vaatama ja hindama teiste asjatundjate tööd ning otsustama nende asjatundjate töö kasutamise ulatuse ja sellele toetumise ulatuse.

06 IS audiitor peaks määrama ja otsustama, kas teiste asjatundjate töö on adekvaatne ja täielik ning võimaldab IS audiitoril teha järelduse käsiloleva auditi eesmärkide kohta. selline järeldus tuleks selgelt dokumenteerida.

07 Olukorras, kus teiste asjatundjate töö ei anna piisavaid ja asjakohaseid auditi asitõendeid, peaks IS audiitor piisavate ja asjakohaste auditi asitõendite saamiseks rakendama täiendavaid testimisprotseduure.

08 Kui täiendavate testimisprotseduuridega ei saada vajalikke asitõendeid, peaks IS audiitor andma asjakohase arvamuse auditi kohta ja lisama käsitlusala kitsenduse.

Lisajuhiseid

09 IS audiitor peaks mõtlema teiste asjatundjate töö kasutamisele auditis, kui on mingeid kitsendusi, mis võiksid kahjustada eelseisvat audititööd, või kui see võib tulla kasuks auditi kvaliteedile. Näiteks juhtudel, kui vajatakse teadmisi eelseisvate audititööde tehnilise iseloomu tõttu või kui auditi ressursid on napid või kui on ajalisi kitsendusi.

10 Asjatundjaks võib olla IS audiitor välisest auditeerimisfirmast, juhtimiskonsultant, IT spetsialist või auditeeritava valdkonna spetsialist, kelle on määranud tippjuhtkond või IS auditi töörühm.

11 Asjatundja võib olla organisatsioonisisene või -väline. Kui asjatundja kaasatakse organisatsiooni teisest osast, tuleb võib-olla toetud tema aruandele. Mõnedel juhtudel võib see vähendada IS auditi katvuse vajadust, ehkki IS audiitoril ei ole juurdepääsu tugidokumentatsioonile ja töödokumentidele. Sellistel juhtudel peaks IS audiitor avaldama oma arvamust ettevaatlikult.

S13 Teiste asjatundjate töö kasutamine (jätkub)

12 IS audiitoril peaks olema juurdepääs kõigile teiste asjatundjate töödokumentidele, tugidokumentatsioonile ja aruannetele, kui selline juurdepääs ei tekita õiguslikke probleeme. Kui asjatundja juurdepääs andmikele tekitab õiguslikke probleeme ja seetõttu puudub, peaks IS audiitor asjakohaselt määrama ja otsustama asjatundja töö kasutamise ulatuse ja sellele toetumise ulatuse.

13 IS audiitori arvamused, seosed ja kommentaarid asjatundja aruande rakendatavuse kohta peaksid moodustama ühe osa IS audiitori aruandest.

14 IS audiitor peaks toetuma IS auditeerimise standardile S6 "Audititöö sooritamine", mis määrab, et IS audiitor peab auditi eesmärkide saavutamiseks hankima piisavad, usaldatavad, asjassepuutuvad ja kasulikud asitõendid.

15 Kui IS audiitoril ei ole auditi sooritamiseks vajalikke oskusi või muud pädevust, peaks ta otsima pädevat abi teistelt asjatundjatelt; IS audiitor peaks aga hästi tundma sooritatavat tööd, ehkki temalt ei eeldata asjatundja omadega võrdseid teadmisi.

16 IS audiitor peaks toetuma IS auditeerimise suunisele G1 "Teiste audiitorite ja asjatundjate töö kasutamine".

17 Lisateabe saamiseks teiste audiitorite ja asjatundjate töö kasutamise kohta tuleks toetuda järgmistele juhistele.

- IS auditeerimise suunised:

  - G5 "Auditikontori põhikiri";

  - G8 "Auditi dokumentatsioon";

  - G2 "Auditi asitõendite nõue";

  - G10 "Valimkontroll auditeerimisel";

  - G13 "Riski kaalutlemise kasutamine auditi plaanimisel";

- COBIT 4.0. IT Halduse Instituut, 2005;
- IT juhtimiseesmärgid Sarbanes-Oxley seaduse osas. IT halduse instituut, 2004.

Jõustumiskuupäev

18 See ISACA standard kehtib kõigi infosüsteemiauditite kohta alates 1. juulist 2006.

S14 Auditi asitõendid

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle standardi eesmärk on kehtestada nõuded ja anda juhiseid selle kohta, mida endast kujutavad auditi asitõendid, ning nende asitõendite kvaliteedi ja koguse kohta, mida peab hankima IS audiitor.

Standard

03 IS audiitor peaks hankima mõistlike järelduste tegemiseks piisavad ja asjakohased auditi asitõendid, millele rajada auditi tulemused.

04 IS audiitor peaks hindama auditi käigus hangitud asitõendite piisavust.

Kommentaarid

Asjakohased asitõendid

05 Auditi asitõendid

- hõlmavad audiitori sooritatud protseduure;
- hõlmavad IS audiitori sooritatud protseduuride tulemusi;
- hõlmavad lähtedokumente (elektroonilisel või paberkujul), andmikke ja auditi abivahendina kasutatavat kinnitavat teavet;
- hõlmavad auditöö leide ja tulemeid;
- tõendavad, et töö sooritati ning vastab kohaldatavatele õigusaktidele, eeskirjadele ja poliitikatele.

06 Kui IS audiitor hangib auditi asitõendeid juhtimismeetmete testimisega, peaks ta hoolitsema selle eest, et auditi asitõendid oleksid juhtimisriski suuruse kohta antud hinnangu toetuseks täielikud.

07 Auditi asitõendid tuleks sobivalt identifitseerida, viitestada ja kataloogida.

08 Auditi asitõendite usaldatavuse hindamisel tuleks arvestada auditi asitõendite selliseid omadusi nagu allikas, iseloom (näiteks: kirjalik, suuline, visuaalne, elektrooniline) ja autentsus (näiteks: digitaalne või käsiallkiri, pitser).

Usaldatavad asitõendid

09 Üldjoontes on auditi asitõendite usaldatavus suurem, kui

- nad on kirjalikul kujul, mitte suulised lausungid;
- nad on saadud sõltumatutest allikatest;
- neid on hankinud IS audiitor, mitte auditeeritav üksus;
- neid tõendab erapooletu osapool;
- nad on sõltumatu osapoole valduses.

S14 Auditi asitõendid (jätkub)

10 IS audiitor peaks kaaluma kõige ökonoomsemaid viise auditi eesmärkide ja riskide seisukohalt vajalike asitõendite kogumiseks. Raskus või kulukus ei ole aga mõjuv põhjus mingi vajaliku protsessi ärajätmiseks.

11 Auditi asitõendite kogumiseks kasutatavad protseduurid varieeruvad sõltuvalt auditeerimisobjektist (st ta iseloomust, auditi ajstusest, kutsealasest otsustusvõimest). IS audiitor peaks valima auditi eesmärgi seisukohalt kõige sobivama protseduuri.

12 IS audiitori käsutuses on auditi asitõendite hankimiseks

- ülevaatus,
- vaatlus,
- küsitlus ja kinnituse saamine,
- kordussooritamine;
- kordusarvutamine;
- andmetöötlus;
- analüütilised protseduurid;
- muud üldtunnustatud meetodid.

13 IS audiitor peaks arvestama igasuguse saadud teabe allikat ja iseloomu, et hinnata selle teabe usaldatavust ja edasise kontrollimise vajadust.

Piisavad asitõendid

14 Asitõendeid võib lugeda piisavaiks, kui nad toetavad kõiki auditi eesmärgi ja käsitlusala seisukohalt kaalukaid küsimusi.

15 Auditi asitõendid peaksid polema objektiivsed ja piisavad selleks, et kvalifitseeritud sõltumatu osapool saaks teste korrata ja jõuda samade tulemusteni. Asitõendid peaksid ulatuselt olema vastavuses küsimuse kaalukusega ja kaasnevate riskidega.

16 Piisavus on auditi asitõendite kvantiteedi mõõt, asjakohasus on aga auditi asitõendite kvaliteedi mõõt ning nad on omavahel seotud. Selles kontekstis tuleb arvestada, et kui IS audiitor kasutab organisatsioonilt saadud teavet auditiprotseduuride sooritamiseks peaks ta pühendama piisavalt tähelepanu selle teabe õigsusele ja täielikkusele.

17 Olukordades, kus IS audiitori arvates ei ole võimalik hankida piisavaid auditi asitõendeid, peaks ta selle fakti avaldama auditi tulemuste teatamisega kooskõlas oleval viisil.

Kaitse ja säilitamine

18 Auditi asitõendeid tuleb kaitsta volitamatu juurdepääsu ja muutmise eest.

19 Auditi asitõendeid tuleks pärast audititöö lõpuleviimist säilitada nii kaua kui on vajalik vastavuseks kohaldatavatele õigusaktidele, eeskirjadele ja poliitikatele

S14 Auditi asitõendid (jätkub)

Teabeallikad

20 Lisateabe saamiseks auditi asitõendite kohta tuleks toetuda järgmistele juhistele:

- IS auditeerimise standard S6 "Auditi töö sooritamine";
- IS auditeerimise suunis G2 "Auditi asitõendite nõue";
- IS auditeerimise suunis G8 "Auditi dokumentatsioon";
- COBITi juhtimiseesmärgid SH2 "Seirata ja hinnata sisejuhtimist" ja SH3 "Tagada vastavus välisnõuetele".

Jõustumiskuupäev

21 See IS auditeerimise standard kehtib kõigi infosüsteemiauditite kohta alates 1. juulist 2006.

S15 IT juhtimismeetmed

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle ISACA standardi eesmärk on kehtestada normid ja anda juhiseid IT juhtimismeetmete kohta.

Standard

03 IS audiitor peaks hindama ja seirama IT juhtimismeetmeid, mis on organisatsiooni sisejuhtimiskeskkonna lahutamatu osa.

04 IS audiitor peaks abistama juhtkonda nõuannetega IT juhtimismeetmete kavandamise, teostamise, käituse ja täiustamise kohta.

Kommentaarid

05 Juhtkond vastutab organisatsiooni sisejuhtimiskeskkonna eest, sealhulgas IT juhtimismeetmete eest. Sisejuhtimiskeskkond loob distsipliini, karkassi ja struktuuri, mille abil saavutada sisejuhtimise süsteemi esmast eesmärki.

06 COBIT määratleb juhtimise nii: "poliitikad, protseduurid, tavad ja organisatsiooni struktuurid, mis on kavandatud andma mõistlikku kinnitust sellele, et tegevusalased eesmärgid saavutatakse ning et soovimatud sündmused välditakse või avastatakse ja heastatakse". COBIT määratleb ka juhtimiseesmärgi: "teatud protsessile juhtimisprotseduuride rakendamise teel taotletava soovitud tulemuse või sihi sõnastus".

07 IT juhtimismeetmed koosnevad üldistest IT juhtimismeetmetest, sealhulgas IT üldmeetmetest, IT detailmeetmetest ja rakenduste meetmetest ning kujutavad endast meetmeid, mida rakendatakse IT-süsteemide ja -teenuste hankimisele, evitamisele, tarnimisele ja toetamisele.

08 Üldised IT juhtimismeetmed on meetmed, mis minimeerivad riski organisatsiooni IT-süsteemide ja infrastruktuuri üldisele talitlusele ja automatiseeritud lahenduste (rakenduste) laiale kogumile.

09 Rakenduste meetmed on rakendustesse ehitatud meetmestik.

10 IT üldmeetmed on üldised IT juhtimismeetmed, mis on kavandatud IT-keskkonna haldamiseks ja seireks ning mis mõjutavad seega kõiki IT-ga seotud tegevusi. Nad on üldiste juhtimismeetmete osahulk, nimelt need üldised IT juhtimismeetmed, mis keskenduvad IT haldusele ja seirele.

11 IT detailmeetmed koosnevad rakenduste meetmetest ja neist üldistest IT juhtimismeetmetest, mis ei kuulu IT üldmeetmete hulka.

12 IS auditi üldise plaani koostamisel ja prioriteetide määramisel IS auditi ressursside toimivaks jaotamiseks eesmärgiga saada kinnitus IT juhtimisprotsesside seisundile peaks IS audiitor kasutama sobivat riski kaalutlemise meetodit või metoodikat. Juhtimisprotsessid on juhtimiskeskkonna üheks osaks olevad poliitikad, protseduurid

S15 IT juhtimismeetmed (jätkub)

ja tegevused, mis on kavandatud tagama riskide jäämise lubatavatesse piiridesse, mis on määratud riskihalduse protsessiga.

13 IS audiitor peaks mõtlema sellele, et kasutada andmeanalüüsi meetodit, mis sisaldab pideva kinnituse rakendamist; see võimaldab IS audiitoril IT juhtimismeetmete läbivaatuse ajal pidevalt jälgida süsteemi usaldatavust ja koguda arvuti kaudu selektiivseid auditi asitõendeid.

14 Kui organisatsioon kasutab kolmandaid osapooli, võivad need omandada otsustava koha organisatsiooni juhtimismeetmetes ja nendega seotud juhtimiseesmärkide saavutamises. IS audiitor peaks hindama rolli, mis kolmandal poolel on IT-keskkonna, sellega seotud juhtimismeetmete ja IT juhtimiseesmärkide suhtes.

15 Lisateabe saamiseks IT juhtimismeetmete kohta tuleks vaadata järgmisi ISACA ja IT Halduse Instituudi (ITGI™) suuniseid:

- Suunis G3 Arvutipõhiste auditimeetodite (CAAT) kasutamine
- Suunis G11 IS üldmeetmete toime
- Suunis G13 Riski kaalutlemise kasutamine auditi plaanimisel
- Suunis G15 Plaanimine
- Suunis G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele
- Suunis G20 Aruandlus
- Suunis G36 Biomeetrilised meetmed
- Suunis G38 Pääsu reguleerimise meetmed
- COBITi raamstruktuur ja juhtimiseesmärgid

Jõustumiskuupäev

16 See ISACA standard kehtib infosüsteemiauditite kohta alates 1. veebruarist 2008.

S16 E-kaubandus

Sissejuhatus

01 ISACA standardid sisaldavad kohustuslikke (need on tähistatud paksu kirjaga) aluspõhimõtteid ja olulisi protseduure koos juurdekuuluvate juhistega.

02 Selle ISACA standardi eesmärk on kehtestada normid ja anda juhiseid IT e-kaubanduse keskkondade läbivaatuse kohta.

Standard

03 E-kaubanduse tehingute juhtimise õigsuses veendumiseks peaks IS audiitor e-kaubanduse keskkondade läbivaatamisel hindama rakendatavaid meetmeid ja kaalutlema riski.

Kommentaarid

04 E-kaubandus määratletakse kui protsess, millega organisatsioonid sooritavad äritegevust oma klientide, tarnijate ja muude väliste äripartneritega elektrooniliselt, kasutades seda võimaldava tehnoloogiana Internetti. Seega hõlmab ta ettevõtetevahelise (B2B)ning ettevõtte ja kliendi vahelise (B2C) e-kaubanduse mudeleid.

05 IS auditi üldise plaani koostamisel peaks IS audiitor kasutama sobivat riski kaalutlemise meetodit või metoodikat, mis kataks ka e-kaubanduse keskkondi.

06 IS audiitor peaks mõtlema sellele, et kasutada andmeanalüüsi meetodit, mis sisaldab pideva kinnituse rakendamist; see võimaldab IS audiitoril e-kaubanduse tegevuste läbivaatuse ajal pidevalt jälgida süsteemi usaldatavust ja koguda arvuti kaudu selektiivseid auditi asitõendeid.

07 Juhtimise ja riskihalduse alaste järelduste mõistmiseks vajalik oskuste ja teadmiste tase sõltub e-kaubanduse puhul organisatsiooni e-kaubanduse tegevuste keerukusest.

08 Enne auditi alustamist peaks IS audiitor õppima tundma e-kaubanduse rakendusega toetatava äriprotsessi iseloomu ja elutähtsust, nii et tulemusi saaks hinnata õiges kontekstis.

09 Lisateabe saamiseks e-kaubanduse kohta tuleks vaadata järgmisi suuniseid:

- Suunis G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus
- Suunis G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus
- Suunis G24 Interneti-pangandus
- Suunis G25 Virtuaalsete privaatvõrkude läbivaatus
- Suunis G33 Interneti kasutamise üldised kaalutlused
- Protseduur P6 Tulemüürid
- COBITi raamstruktuur ja juhtimiseesmärgid

Jõustumiskuupäev

10 See ISACA standard kehtib infosüsteemiauditite kohta alates 1. veebruarist 2008.

Infosüsteemide auditeerimise suunised

Infosüsteemide auditeerimise suuniste tähestikloend

Infosüsteemide auditeerimise suunised

G1 Teiste spetsialistide töö kasutamine

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S13 "Teiste spetsialistide töö kasutamine" määrab: "Asjakohastel juhtudel peaks IS audiitor mõtlema teiste spetsialistide töö kasutamisele auditis."

1.1.2 Standard S6 "Auditi töö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.2 Seos COBITiga

1.2.1 SH2.5 määrab, et IS audiitor peaks „vajadusel saama sisemeetmete täielikkuse ja toimivuse kohta lisakinnitust kolmanda poole sooritatud läbivaatustega. Selliseid läbivaatusi võib läbi viia organisatsiooni vastavustalitus või juhtkonna tellimusel siseaudit või need võidakse tellida välisaudiitoritelt ja -konsultantidelt või sertifitseerimisorganitelt. Peab olema tagatud auditit sooritavate isikute kvalifikatsioon, näiteks CISA® sertifitseering.“

1.3 Suunise vajadus

1.3.1 Klientide ja tarnijate protsesside vastastikuse sõltuvuse ning kõrvalisemate tegevuste väljasttellimise tõttu avastab (sisemine või väline) IS audiitor sageli, et auditeeritava keskkonna mingeid osi juhivad ja auditeerivad muud sõltumatud talitused või organisatsioonid. Käesolev suunis seletab, kuidas peaks IS audiitor niisuguses olukorras järgima ülalnimetatud standardit. Vastavus sellele suunisele ei ole kohustuslik, kuid IS audiitor peaks olema valmis põhjendama sellest lahknemist.

1.3.2 IS audiitorid peaksid mõtlema teiste spetsialistide töö kasutamisele auditis, kui on mingeid kitsendusi, mis võiksid kahjustada sooritatavat auditi tööd, või kui sellest võib oodata auditi kvaliteedi tõusu. Niisuguste põhjuste näited on sooritamisele kuuluvate tööde tehnilise iseloomu tõttu vajalikud teadmised, auditi napid ressursid, auditi spetsiifiliste alade puudulik tundmine. Spetsialistiks võib olla IS audiitor välisest auditeerimisfirmast, juhtimiskonsultant, IT-spetsialist või auditeeritava ala spetsialist, kelle on määranud tippjuhtkond või IS auditi töörühm. Spetsialist võib olla organisatsioonisisene või -väline, kuid ta peab säilitama sõltumatuse ja objektiivsuse.

G1 Teiste spetsialistide töö kasutamine (jätkub)

2 AUDITI PÕHIKIRI

2.1 Õigused juurdepääsuks teiste spetsialistide tööle

2.1.1 IS audiitor peaks veenduma, et juhuks, kui IS auditi eesmärke puudutab ka teiste spetsialistide töö, spetsifitseerib auditi põhikiri või töövõtukiri IS audiitori õiguse juurdepääsuks sellele tööle.

3 PLAANIMINE

3.1 Plaanimiskaalutlused

3.1.1 Kui IS audiitoril ei ole auditi sooritamiseks vajalikke oskusi või muud pädevust, peaks ta otsima pädevat abi teistelt spetsialistidelt; IS audiitor peaks küll hästi tundma sooritatavat tööd, kuid temalt ei saa oodata spetsialistidega võrdset teadmiste taset.

3.1.2 Kui IS audit sisaldab teiste spetsialistide töö kasutamist, peaks IS audiitor IS auditi töö plaanimisel arvestama nende tegevust ja selle mõju IS auditi eesmärkidele. Plaanimisprotsessi koostisse peaksid kuuluma

- teiste spetsialistide sõltumatuse ja objektiivsuse otsustamine;
- nende kutsealase pädevuse ja kvalifikatsiooni otsustamine;
- nende töö käsitlusala, metoodika, ajastuse ja kvaliteedikujunduse protsesside tundmaõppimine, sealhulgas otsustamine, kas nad olid piisavalt hoolikad töödokumentide koostamisel ja oma töö asitõendite säilitamisel;
- vajaliku läbivaatuse taseme määramine.

3.2 Sõltumatus ja objektiivsus

3.2.1 Teiste spetsialistide sõltumatuse ja objektiivsuse näitajad on valimise ja määramise protsessid, organisatsiooniline staatus, alluvusliin ja nende isikute soovituste mõju juhtimistavadele.

3.3 Kutsealane pädevus

3.3.1 Teiste spetsialistide kutsealase pädevuse otsustamisel tuleks arvestada nende kvalifikatsiooni, kogemust, ressursse ja tunnistusi.

3.4 Töö käsitlusala ja meetodid

3.4.1 Töö käsitlusala ja meetodid ilmnevad tavaliselt teiste spetsialistide kirjalikust auditi põhikirjast, volitusalast või töövõtukirjast.

G1 Teiste spetsialistide töö kasutamine (jätkub)

3.5 Vajalik läbivaatuse tase

3.5.1 Vajalike auditi asitõendite iseloom, ajastus ja maht sõltub teiste spetsialistide töö tähtsusest. IS audiitori plaanimisprotsess peaks piiritlema läbivaatuse taseme, mis on vajalik kõigi IS auditi eesmärkide toimivaks saavutamiseks piisavate usaldatavate, asjassepuutuvate ja kasulike auditi asitõendite saamiseks. IS audiitor peaks läbi vaatama teiste spetsialistide lõpparuande, auditi kava(d) ja auditi töödokumendid. IS audiitor peaks mõtlema ka sellele, kas on vaja täiendavalt kontrollida teiste spetsialistide tööd.

4 AUDITITÖÖ SOORITAMINE

4.1 Teise spetsialisti töödokumentide läbivaatus

4.1.1 IS audiitoril peaks olema juurdepääs kõigile spetsialisti koostatud töödokumentidele, mis toetavad teiste spetsialistide dokumentatsiooni ja aruandeid, kui selline juurdepääs ei tekita õigusprobleeme.

4.1.2 Kui spetsialisti juurdepääs andmikele tekitab õigusprobleeme ja pole seetõttu võimalik, peaks IS audiitor sobivalt määrama ja otsustama spetsialisti töö kasutamise ja sellele toetumise ulatuse.

4.1.3 Teise spetsialisti töödokumentide läbivaatamisel peaks IS audiitor sooritama piisavalt audititööd kinnituse saamiseks sellele, et teise spetsialisti tööd plaaniti, jälgiti, dokumenteeriti ja vaadati läbi asjakohaselt tema hangitud asitõendite asjakohasuse ja piisavuse määramiseks ning spetsialisti töö kasutamise ja sellele toetumise ulatuse otsustamiseks. Tuleks otsustada ka vastavus asjassepuutuvatele kutseala standarditele. IS audiitor peaks otsustama, kas teiste spetsialistide töö on adekvaatne ja täielik võimaldama IS audiitoril teha järeldust käimasoleva auditi eesmärkide kohta ja neid järeldusi dokumenteerida.

4.1.4 Olukorras, kus teiste spetsialistide töö ei anna piisavaid ja sobivaid auditi asitõendeid, peaks IS audiitor teiste spetsialistide töödokumentide hindamise põhjal rakendama piisavate ja sobivate auditi asitõendite saamiseks täiendavaid kontrollimisprotseduure.

4.1.5 Kui täiendavad kontrollimisprotseduurid ei anna piisavaid ja sobivaid auditi asitõendeid, peaks IS audiitor tegema sellekohase auditijärelduse ning vajadusel lisama käsitlusala kitsenduse.

4.2 Teise spetsialisti aruannete läbivaatus

4.2.1 IS audiitor peaks sooritama piisavaid teise spetsialisti lõpparuannete läbivaatusi kinnituse saamiseks sellele, et auditi põhikirjas, volitusalas või töövõtukirjas spetsifitseeritud käsitlusala on järgitud, et kõik olulised teise spetsialisti rakendatud eeldused on välja selgitatud, ning et juhtkond on kinnitanud aruandes esitatud leiud ja järeldused.

G1 Teiste spetsialistide töö kasutamine (jätkub)

4.2.2 Juhtkonnale võib osutuda sobivaks esitada auditeeritavate üksuste kohta omaenda aruanne, mõistes oma esmast vastutust sisejuhtimise süsteemide eest. Sellisel juhul peaks IS audiitor vaatlema juhtkonna ja spetsialisti aruandeid koos.

4.2.3 IS audiitor peaks tegema otsuse teiste spetsialistide aruannete kasulikkuse ja asjakohasuse kohta ning arvestama kõiki nende teatatud olulisi leide. IS audiitori kohus on otsustada, milline on teise spetsialisti leidude ja järelduste mõju auditi üldeesmärgile, ja kontrollida, kas kõik auditi üldeesmärgi saavutamiseks vajalikud lisatööd on lõpule viidud.

4.2.4 Kui organisatsiooni mingi teine osa on palganud spetsialisti, võib toetuda selle spetsialisti aruandele. Mõnedel juhtudel võib see vähendada IS auditi katvuse vajadust, ehkki IS audiitoril ei ole juurdepääsu tugidokumentatsioonile ja töödokumentidele. IS audiitor peaks sellistel juhtudel olema arvamuse avaldamisel ettevaatlik.

4.2.5 Kui IS audiitor kasutas oma arvamuse kujundamisel spetsialisti aruannet, peaksid IS audiitori ühe osa moodustama IS audiitori seisukohad ja kommentaarid spetsialisti aruande rakendatavuse ja asjassepuutuvuse kohta.

5 JÄRELTOIMINGUD

5.1 Soovituste elluviimine

5.1.1 Asjakohastel juhtudel peaks IS audiitor mõtlema sellele, millises ulatuses on juhtkond viinud ellu teiste spetsialistide soovitusi. Seejuures tuleks tal otsustada, kas juhtkond on asunud sobivates ajapiirides lahendama teiste spetsialistide tuvastatud probleeme, ning hinnata lahendamise hetkeseisu.

6 JÕUSTUMISKUUPÄEV

6.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. juunil 1998 või pärast seda. Läbivaadatud ja ajakohastatud suunis jõustub 1. märtsil 2008.

G2 Auditi asitõendite nõue

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Auditit öö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.2 Standard S9 "Korratused ja ebaseaduslikud toimingud" määrab: "IS audiitor peaks hankima piisavaid ja asjakohaseid auditi asitõendeid otsustamiseks, kas juhtkond või muud organisatsiooni kuulujad teavad mingeid tegelikke, kahtlustatavaid või oletatavaid korratusi või ebaseaduslikke toiminguid."

1.1.3 Standard S13 "Teiste spetsialistide töö kasutamine" määrab: "Kui täiendavate testimisprotseduuridega ei saada vajalikke asitõendeid, peaks IS audiitor andma asjakohase arvamuse auditi kohta ja lisama käsitlusala kitsenduse."

1.1.4 Standard S14 " Auditi asitõendid " määrab: "IS audiitor peaks hankima mõistlike järelduste tegemiseks piisavad ja asjakohased auditi asitõendid, millele rajada auditi tulemused. IS audiitor peaks hindama auditi käigus hangitud asitõendite piisavust."

1.1.5 Protseduur P7 "Korratused ja ebaseaduslikud toimingud" määrab: "Kuigi IS audiitor ei ole otseselt kohustatud avastama või vältima korratusi, peaks ta kaalutlema korratuste toimumise riski suurust. Ülesande täitmise ajal sooritatavate protseduuride iseloomu, ulatuse ja ajastuse määramiseks tuleks kasutada riski kaalutlemise ja muude plaanimise ajal sooritatud protseduuride tulemusi.

1.2 Seos COBITiga

1.2.1 SH2.3 "Ohjata erandeid" määrab: "Jäädvustada teavet kõigi juhtimiserandite kohta ning tagada, et see viiks erandi põhjuse analüüsini ja parandusmeetmeteni. Juhtkond peaks otsustama, millistest eranditest tuleks teatada tegevusliini eest vastutavale isikule ja milliste erandite käsitlust tuleks laiendada. Juhtkonna kohus on ka teavitada mõjutatavaid pooli.

1.3 Suunise vajadus

1.3.1 Selle suunise eesmärk on juhendada IS audiitorit piisavate ja sobivate auditi asitõendite hankimisel ja mõistlike järelduste tegemisel, millele rajada auditi tulemused.

1.3.2 See suunis annab juhiseid IS auditeerimise standardite rakendamise kohta. IS audiitor peaks seda järgima otsustamisel, kuidas saavutada ülalnimetatud standardi elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

G2 Auditi asitõendite nõue (jätkub)

2 PLAANIMINE

2.1 Auditi asitõendite tüübid

2.1.1 Sobivaid, usaldatavaid ja piisavaid asitõendeid kirjeldab standardi S14 kommentaariosa.

2.1.2 IS audititöö plaanimisel peaks IS audiitor arvestama kogumisele kuuluvate auditi asitõendite tüüpi, nende asitõendite kasutamist auditi eesmärkide saavutamiseks ja nende kõikuvat usaldatavuse taset. Peale selle tuleb arvestada auditi asitõendite andja sõltumatust ja oskusi. Näiteks võivad sõltumatult kolmandalt poolelt saadud kinnitavad auditi asitõendid olla usaldusväärsemad kui auditeeritavalt organisatsioonilt saadud asitõendid. Füüsilised auditi asitõendid on üldiselt inimeste seletustest usaldusväärsemad.

2.1.3 IS audiitor peaks mõtlema ka sellele, kas meetmete testimine on lõpetatud ja kas seda on tõendanud sõltumatu kolmas pool ning kas sellel testimisele saab toetuda.

2.1.4 IS audiitor peaks kaaluma muuhulgas järgmiste asitõenditüüpide kasutamist:

- vaadeldavad protsessid ja füüsiliste tõendite olemasolu;
- dokumentaalsed auditi asitõendid;
- teabeesitused;
- analüüs.

2.1.5 Vaadeldavad protsessid ja füüsiliste tõendite olemasolu võivad hõlmata tegevuste, omandi ja infosüsteemide talitluse vaatlusi, näiteks

- väljaspool tegevuskohta ladustatud infokandjate inventeerimist,
- arvutiruumi turvasüsteemi tööd.

2.1.6 Paberil või muul kandjal jäädvustatud dokumentaalsete auditi asitõendite hulka võivad kuuluda

- andmevõttude tulemused,
- tehingute andmikud,
- programmilistingud,
- arved,
- tegevuste ja juhtimise logid,
- süsteemiarenduse dokumentatsioon.

2.1.7 Auditi asitõenditeks võivad olla audieeritavate teabeesitused, näiteks

- kirjalikud poliitikad ja protseduurid,
- süsteemide vooskeemid,
- kirjalikud või suulised väited.

G2 Auditi asitõendite nõue (jätkub)

2.1.8 Auditi asitõenditena saab kasutada ka võrdlemise, simuleerimise, arvutuste ja järeldamise teel sooritatava teabeanalüüsi tulemusi. Näiteks võib

- mõõdelda IS sooritust teiste organisatsioonide või eelmiste perioodidega võrreldes;
- võrrelda eri rakenduste, tehingute või kasutajate veasagedusi.

2.2 Auditi asitõendite käideldavus

2.2.1 IS audiitor peaks olulisuse (ja asjakohasel juhul ka vastavuse) kontrollimise iseloomu, ajastuse ja ulatuse määramisel võtma arvesse aega, mille kestel teave on olemas või kättesaadav. Kui auditi asitõendeid töödeldakse näiteks EDI-andmevahetuse, dokumentide rastertöötluse (DIP) või dünaamilise (näiteks arvutustabelite) süsteemiga, võivad nad pärast mingit ettemääratud ajavahemikku olla kättesaamatud, kui failide muudatusi ei ohjata või kui ei tehta failide varukoopiaid. Dokumentide käideldavust võiksid rõhutada ka ettevõtte dokumendisäilituse poliitikad.

2.3 Auditi asitõendite valimine

2.3.1 IS audiitor peaks plaanima kõige sobivamate, usaldatavamate ja piisavamate kättesaadavate auditi asitõendite kasutamise, nii et need oleksid kooskõlas auditi eesmärgi tähtsusega ning asitõendite hankimise aja- ja töökuluga.

2.3.2 Kui suulise esituse kujul saadud asitõendid on auditi arvamuse või järelduse seisukohalt väga olulised, peaks IS audiitor kaaluma sellele esitusele dokumentaalse kinnituse saamist paberil või muul infokandjal.

3 AUDITITÖÖ SOORITAMINE

3.1 Auditi asitõendite iseloom

3.1.1 Arvamuse kujundamiseks või IS audiitori leidude ja järelduste toetamiseks peaksid auditi asitõendid olema piisavad, usaldatavad, asjassepuutuvad ja kasulikud arvamuse kujundamiseks või IS audiitori leidude ja järelduste toetuseks. Kui hangitud asitõendid IS audiitori arvates ei rahulda neid kriteeriume, peaks ta hankima täiendavaid auditi asitõendeid. Näiteks ei tarvitse programmilisting olla adekvaatne auditi asitõend, enne kui on kogutud muid asitõendeid, millega kontrollida, kas ta esitab tegelikku tootmisprotsessis kasutatavat programmi.

G2 Auditi asitõendite nõue (jätkub)

3.2 Auditi asitõendite kogumine

3.2.1 Auditi asitõendite kogumiseks kasutatavad protseduurid varieeruvad sõltuvalt auditeeritavast infosüsteemist. IS audiitor peaks valima auditi eesmärgi seisukohalt kõige sobivama protseduuri. Arvestada tuleks järgmisi protseduure:

- küsitlus,
- vaatlus,
- ülevaatus,
- kinnitus,
- kordussooritus,
- seire.

3.2.2 Ülalloetletut võib rakendada auditi käsiprotseduuride, arvutipõhiste auditeerimismeetodite või nende kombinatsiooni kasutamise teel. Seda illustreerivad järgnevad näited.

- Süsteem, kus kasutatakse andmesisestusoperatsioonide kontrollimiseks käsitsi arvutatavaid kontrollsummasid, võiks auditi asitõendeid kontrolliprotseduuride olemasolu kohta anda sobivalt kõrvutava ja kommenteeriva aruande kaudu. IS audiitor peaks hankima auditi asitõendeid selle aruande läbivaatuse ja kontrollimise teel.
- Üksikasjalikud tehinguandmikud võivad olemas olla ainult masinloetaval kujul ja sel juhul tuleb IS audiitoril hankida auditi asitõendeid arvutipõhiste auditeerimismeetoditega. Audiitor peaks hoolitsema selle eest, et kasutatavate CAAT-vahendite (arvutipõhiste auditeerimisvahendite) versioonid või tüübid oleksid ajakohastatud ja/või täielikult ühilduksid kõnealuste detailsete tehinguandmike jaoks struktureeritud vormingu(te)ga.

3.2.3 Kui on olemas võimalus, et kogutud asitõendeid kasutatakse kohtumenetluses, peaks IS audiitor konsulteerima sobiva juristiga otsustamaks, kas on mingeid erinõudeid, mis mõjutavad seda, kuidas tuleb asitõendeid koguda, esitada ja avaldada.

3.3 Auditi dokumenteerimine

3.3.1 IS audiitori kogutud asitõendid tuleks asjakohaselt dokumenteerida ja süstematiseerida, nii et nad toetaksid IS audiitori leide ja järeldusi.

3.3.2 Asitõendite kaitsmist ja säilitamist käsitleb standardi S14 kommentaariosa.

G2 Auditi asitõendite nõue (jätkub)

4 ARUANDLUS

4.1 Käsitlusala kitsendus

4.1.1 Olukordades, kus IS audiitori arvates ei saa hankida piisavaid auditi asitõendeid, peaks IS audiitor tegema selle fakti teatavaks auditi tulemustest teatamisega kooskõlas oleval viisil.

5 JÕUSTUMISKUUPÄEV

5.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. detsembril 1998 või pärast seda. Läbivaadatud ja ajakohastatud suunis jõustub 1. mail 2008.

G3 Arvutipõhiste auditimeetodite (CAAT) kasutamine

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite sobiva analüüsi ja tõlgendamisega"

1.1.2 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.3 Standard S3 "Kutse-eetika ja standardid" määrab: "Auditiülesannete täitmisel peaks IS audiitor ilmutama kutsealast hoolikust, sealhulgas järgima kohaldatavaid kutsealaseid auditeerimise standardeid."

1.1.4 Standard S7 "Aruandlus" määrab: "IS audiitoril peaksid aruandes esitatud tulemuste toetuseks olema piisavad ja asjakohased auditi asitõendid."

1.1.5 Standard S14 "Auditi asitõendid" määrab: "IS audiitor peaks hankima mõistlike järelduste tegemiseks piisavad ja asjakohased auditi asitõendid, millele rajada auditi tulemused."

1.2 Seos suunistega

1.2.1 Suunis G2 "Auditi asitõendite nõue" annab IS audiitorile juhiseid IS auditeerimisel kasutatavate auditi asitõendite tüübi ja piisavuse kohta.

1.2.2 Suunis G10 "Valimkontroll auditeerimisel" annab IS audiitorile juhiseid auditi valimi kavandamise ja võtu kohta ning valimivõtu tulemuste hindamise kohta.

1.3 Seos COBITiga

1.3.1 SH2 "Seirata ja hinnata sisejuhtimist" rahuldab ärinõuet IT-le: kaitsta IT eesmärkide saavutamist ja järgida IT-ga seotud õigusakte, keskendudes selleks IT-ga seotud tegevuste sisejuhtimise protsesside seirele ja piiritledes täiustusmeetmed.

1.3.2 TT5 "Tagada süsteemide turvalisus" rahuldab ärinõuet IT-le: säilitada teabe ja töötluse infrastruktuuri terviklus ning minimeerida turvanõrkuste ja -intsidentide toimet, keskendudes infoturbe poliitikate, protseduuride ja standardite määratlemisele ning turvanõrkuste ja -intsidentide seirele, avastamisele, teatavakstegemisele ja lahendamisele.

1.4 Suunise vajadus

1.4.1 Sedamööda, kuidas äriüksused üha enam kasutavad andmete jäädvustuseks, edastuseks töötluseks infosüsteeme, muutub auditi katvuse lahutamatuks osaks IS audiitori vajadus kasutada riski adekvaatseks kaalutlemiseks IS-instrumente.

G3 Arvutipõhiste auditimeetodite (CAAT) kasutamine (jätkub)

Arvutipõhised auditimeetodid (CAAT) on IS audiitorile tähtsad töövahendid juhtimiskeskkonna tõhusaks ja toimivaks hindamiseks. CAAT-vahendite kasutamine võib võimaldada auditi suuremat katvust, andmete põhjalikumat ja järjekindlamat analüüsi ning riski vähenemist.

1.4.2 CAAT hulka kuuluvad mitmesugust tüüpi instrumendid ja meetodid, näiteks üldistatud auditi tarkvara, individualiseeritud päringud ja skriptid, utiliidid, rakendustarkvara jälitus ja vastendus ning auditeerimise ekspertsüsteemid.

1.4.3 CAAT-vahendeid võib kasutada mitmesuguste auditi protseduuride sooritamisel; selliste hulka kuuluvad

- tehingute ja bilansside üksikasjade kontrollid,
- analüütilised läbivaatuse protseduurid,
- IS üldiste ohjemeetmete vastavuse kontrollid,
- IS rakenduste ohjemeetmete vastavuse kontrollid,
- läbistustestimine.

1.4.4 CAAT-vahendid võivad luua suure osa asitõenditest, mis kogunevad IS auditite käigus, seetõttu peaks IS audiitor nende vahendite kasutamist hoolikalt plaanima ja ilmutama nende kasutamisel asjakohast kutsealast hoolikust.

1.4.5 See suunis annab juhiseid IS auditeerimise standardite rakendamiseks. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardite elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

1.4.6 Neid juhiseid tuleks kohaldada CAAT-vahendite kasutamisel sõltumata sellest, kas neid kasutav audiitor on IS audiitor.

2 PLAANIMINE

2.1 CAAT-vahendite kasutamist määravad tegurid

2.1.1 Auditi plaanimisel peaks IS audiitor mõtlema käsimeetodite ja CAAT-vahendite sobivale kombinatsioonile. CAAT-vahendite kasutamise otsustamisel tuleks võtta arvesse järgmised tegurid:

- IS audiitori arvutioskus, arvutialane asjatundmine ja kogemus,
- sobivate CAAT- ja IS-vahendite olemasolu;
- CAAT-vahendite tõhusus ja toimivus käsimeetoditega võrreldes;
- ajalised kitsendused;
- infosüsteemi ja IT-keskkonna terviklus;
- auditiriski tase.

G3 Arvutipõhiste auditimeetodite (CAAT) kasutamine (jätkub)

2.2 CAAT-vahendite plaanimise sammud

2.2.1 IS audiitori peamiste sammude hulka, mis tal tuleb läbida väljavalitud CAAT-vahendite rakendamise ettevalmistamisel, kuuluvad järgmised:

- seada CAAT-vahenditele auditi eesmärgid; need võivad sisalduda auditiülesande lähtetingimustes;
- määrata organisatsiooni IS-vahendite, programmide, süsteemide ja andmete juurdepääsetavus ja olemasolu;
- teha endale selgeks töödeldavate andmete koostis, sealhulgas kogus, tüüp, vorming ja paigutus;
- määratleda sooritatavad protseduurid (näiteks: statistiline valimivõtt, ülearvutamine, kinnitamine jm);
- määratleda nõuded tulemitele;
- määrata ressursivajadused, näiteks: personal, CAAT-vahendid, töötluskeskkond (organisatsiooni IS vahendid või auditi IS vahendid);
- saada juurdepääs organisatsiooni IS vahenditele, programmidele, süsteemidele ja andmetele, sealhulgas failimääratlustele;
- dokumenteerida kasutamisele kuuluvad CAAT-vahendid, sealhulgas eesmärgid, üldisel tasemel vooskeemid ja käitusjuhendid.

2.3 Ettevalmistused auditeeritava juures

2.3.1 CAAT-vahendite õigeks kavandamiseks ja andmete tõlgendamiseks tuleb andmete omanikel või kasutajatel võib-olla kulutada piisavalt aega. Peale selle peaks auditeeritav tundma CAAT-vahendite otstarvet, käsitlusala, ajastust ja sihte. Algusest peale tuleks tekitada selged ootused CAAT-vahendite suhtes.

2.3.2 Andmefaile, näiteks üksikasjalikke tehingufaile, säilitatakse sageli ainult väga lühikest aega; seetõttu peaks IS audiitor leppima kokku andmete säilitamise aja, mis kataks auditi jaoks sobiva ajavahemiku.

2.3.3 Juurdepääs organisatsiooni IS vahenditele, programmidele, süsteemidele ja andmetele tuleks organisatsiooni tootmiskeskkonna mõjutamise minimeerimiseks kokku leppida juba varakult enne vajalikku ajavahemikku.

2.3.4 IS audiitor peaks kaalutlema tootmisprogrammide ja -süsteemi muutuste võimalikku mõju CAAT-vahendite kasutamisele. Seejuures peaks ta mõtlema sellele, kuidas need muudatused võivad mõjutada CAAT-vahendite terviklust ja kasulikkust ning nende programmide, süsteemide ja andmete terviklust, mida kasutab IS audiitor.

G3 Arvutipõhiste auditimeetodite (CAAT) kasutamine (jätkub)

2.4 CAAT-vahendite testimine

2.4.1 On väga oluline, et IS audiitor saaks mõistliku kinnituse CAAT-vahendite terviklusele, usaldatavusele, kasulikkusele ja turvalisusele asjakohase plaanimise, kavandamise, testimise, töötluse ja dokumentatsiooni läbivaatusega. Alles pärast seda võib ta toetuda CAAT-vahenditele. Testimise iseloom, ajastus ja ulatus sõltub CAAT-vahendite kaubanduslikust kättesaadavusest ja stabiilsusest. Kohandatud CAAT-vahendite ootuspärases töötamises veendumiseks tuleks neid täiendavalt läbi vaadata ja testida.

2.5 Andmete ja CAAT-vahendite turvalisus

2.5.1 Kui CAAT-vahendeid kasutatakse teabe väljaeraldamiseks andmete analüüsi eesmärgil, peaks IS audiitor kontrollima selle infosüsteemi ja IT-keskkonna terviklust, millest need andmed võetakse.

2.5.2 CAAT-vahenditega võidakse välja eraldada tundlikku programmi- ja süsteemiteavet ning tootmisandmeid, mida tuleks hoida konfidentsiaalsetena. IS audiitor peaks sellise programmi- ja süsteemiteabe ning tootmisandmed kaitsma asjakohase konfidentsiaalsus- ja turvatasemega. Seejuures peaks ta arvestama konfidentsiaalsus- ja turvataset, mida nõuavad organisatsioon, kellele andmed kuuluvad, ja kohaldatavad õigusaktid, ning vajadusel pidama nõu teistega, näiteks juristiga või juhtkonnaga. .

2.5.3 CAAT-vahendite pideva tervikluse, usaldatavuse, kasulikkuse ja turvalisuse tagamiseks peaks IS audiitor kasutama sobivaid protseduure ja dokumenteerima nende tulemused. Näiteks peaks nende hulka kuuluma sisseehitatud audititarkvara hoolduse ja muutmise turvameetmete läbivaatus, millega saab teha kindlaks, kas CAAT-vahendites on tehtud ainult lubatavaid muudatusi.

2.5.4 Kui CAAT-vahendid asuvad keskkonnas, mis ei ole IS audiitori kontrolli all, tuleks rakendada asjakohasel tasemel meetmeid, millega tuvastada muutused CAAT-vahendites. CAAT-vahendite muutumise korral peaks IS audiitor enne neile toetumist veenduma nende tervikluses, usaldatavuses, kasulikkuses ja turvalisuses asjakohase plaanimise, kavandamise, testimise, töötluse ja dokumentatsiooni läbivaatusega.

3 AUDITITÖÖ SOORITAMINE

3.1 Auditi asitõendite kogumine

3.1.1 IS audiitor peaks ohjama CAAT-vahendite kasutamist mõistliku kinnituse saamiseks sellele, et kasutamine vastab auditi eesmärkidele ja CAAT-vahendite detailsetele spetsifikatsioonidele. IS audiitor peaks

- sobivatel juhtudel võrdlema kontrollsummasid;
- vaatama läbi tulemid nende mõistlikkuse kontrollimiseks;

- vaatama läbi CAAT-vahendite loogika, parameetrid või muud tunnusomadused;
- vaatama läbi organisatsiooni üldised IS turvameetmed, mis võivad aidata säilitada CAAT-vahendite terviklust (näiteks programmide muutmise meetmed ning juurdepääs süsteemi-, programmi- ja andmefailidele).

3.1.2 Testandmete kasutamisel peaks IS audiitor olema teadlik sellest, et testandmed ainult näitavad vigase töötluse võimalusi; see meetod ei hinda tegelikke tootmisandmeid. IS audiitor peaks teadma ka seda, et testandmete analüüs võib sõltuvalt töödeldavate tehingute arvust, testitavate programmide arvust ning programmide ja süsteemide keerukusest olla äärmiselt keeruline ja aeganõudev. Enne testandmete kasutamist peaks IS audiitor kontrollima, kas testandmed ei mõjuta tegelikku töösüsteemi püsivalt.

3.2 Üldistatud auditi tarkvara

3.2.1 Kui üldistatud auditi tarkvara kasutatakse tootmisandmete poole pöördumiseks, peaks IS audiitor rakendama asjakohaseid abinõusid organisatsiooni andmete tervikluse kaitseks. Sisseehitatud auditi tarkvara puhul peaks IS audiitor osalema süsteemi projekteerimises ning meetodite väljatöötamine ja hooldus peaks toimuma organisatsiooni rakendusprogrammide või -süsteemide raames.

3.3 Utiliidid

3.3.1 Utiliitide kasutamisel peaks IS audiitor veenduma, et töötluse ajal ei ole aset leidnud plaanivälised sekkumised ja et utiliidid on saadud asjakohasest süsteemiteegist. IS audiitor peaks ka rakendama sobivaid abinõusid organisatsiooni süsteemi ja failide kaitseks, sest sellised utiliidid võivad hõlpsasti kahjustada süsteeme ja ta faile.

3.4 Individualiseeritud päringud ja skriptid

3.4.1 Individualiseeritud päringud ja skriptid võimaldavad IS audiitoril võtta spetsiifiliselt vaatluse alla soovitud teabe selle analüüsimiseks. Individualiseeritud skriptidest on palju kasu keskkondades, mille jaoks muid CAAT-vahendeid ei ole, kuid harilikult nõuab nende loomine spetsiifiliste tehniliste oskuste kombinatsioone. Seetõttu peaks IS enne toetumist CAAT-vahenditele saama sobiva plaanimise, kavandamise ja testimisega kinnituse nende tervikluse, usaldatavuse ja turvalisuse kohta ning hoolitsema selle eest, et kasutataks õigeid lähteandmeid ja et skriptide ja päringute väljundandmed oleksid õiges vormingus. Lubamatute muudatuste vältimiseks tuleks individualiseeritud päringute ja skriptide koodi hoida turvalises kohas.

G3 Arvutipõhiste auditimeetodite (CAAT) kasutamine (jätkub)

3.5 Rakendustarkvara jälitamine ja vastendamine

3.5.1 Rakendustarkvara jälitamise ja vastendamise kasutamisel peaks IS audiitor veenduma selles, et hindamisel olev lähtekood genereeris objektprogrammi, mida hetkel kasutatakse tootmises. IS audiitor peaks olema teadlik sellest, et rakendustarkvara jälitamine ja vastendamine ainult osutab vigase töötluse võimalusele ega hinda tegelikke tootmisandmeid.

3.6 Auditeerimise ekspertsüsteemid

3.6.1 Auditeerimise ekspertsüsteemid on spetsialiseeritud instrumendid, mida saab kasutada rakendustarkvara töötlusloogikat läbiva andmevoo analüüsimiseks ning loogika, teede, juhtimistingimuste ja töötlusjadade dokumenteerimiseks. Auditeerimise ekspertsüsteemide kasutamisel peaks IS audiitor põhjalikult tundma süsteemi tööd, nii et ta saaks kinnitada, et järgitud otsustusteed on konkreetses auditi keskkonnas või olukorras asjakohased.

3.7 Pidev seire ja kontroll

3.7.1 Pidev kontroll on katkematu seire meetod, mis võimaldab juhtkonnal ja IS audiitoritel pidevalt seirata juhtimismeetmeid ja koguda arvuti kaudu valikulisi auditi asitõendeid. Seda protsessi saavad IS audiitorid kasutada viivitamatuks (või peaaegu viivitamatuks) aruandluseks ning teda saab kasutada suureriskilistes suuremahulistes keskkondades. Praeguses auditi mudelis (mida kasutavad nii sise- kui ka välisaudiitorid) möödub välitöö lõpetamisest sellega seotud aruande väljastuseni teatav ajavahemik. Paljudel juhtudel on aruandes sisalduvast teabest sellise hilistumise tõttu kasutajale vähem kasu. See tuleneb aruandes sisalduva teabe vananemisest; teavet võib mõjutada näiteks see, et auditeeritav on kõrvaldanud tuvastatud puudusi või et on jätkunud juhtimiskeskkonna (või auditeeritava sellega seotud andmete) laostumine juba tuvastatud juhtimisnõrkuste või -puuduste tõttu.

3.7.2 Niisiis on pidev kontroll kavandatud võimaldama IS audiitoritel esitada käsitletava ala kohta aruandeid palju lühema hilistusega kui praeguse mudeli puhul. Teoreetiliselt peaks mõnedes keskkondades olema võimalik lühendada aruandluse hilistust nii, et kontroll on peaaegu viivitamatu või tõeliselt pidev.

3.7.3 Määratluse järgi nõuab pidev kontroll tugevamat sõltuvust auditeeritava infosüsteemidest kui traditsiooniline auditeerimine. See tuleneb vajadusest toetuda auditeerimistestimisel mitte väljaspool loodud teabele, vaid süsteemi genereeritavale teabele. Seetõttu tuleb audiitoritel teha otsustusi nii auditeeritava süsteemide kvaliteedi kui ka süsteemi loodava teabe enda kohta. Madalakvaliteedilised või vähemusaldatavat teavet loovad (ja suuremal määral käsitsi sekkumist nõudvad) süsteemid sobivad pidevaks kontrolliks vähem kui kvaliteetsed ja usaldatavat teavet loovad süsteemid.

3.7.4 Aruandluseks lühikese kuni pideva kestusega perioodide kohta sobivad paremini kvaliteetsed ja usaldatavat teavet andvad keskkonnad. Madalama kvaliteediga või vähemusaldatavat teavet andvad keskkonnad peaksid kasutama pikemaid aruandlusperioode, nii et korvataks ajavahemik, mis kulub kasutajail süsteemiga töödeldud teabe läbivaatuseks ja kinnitamiseks või parandamiseks.

G3 Arvutipõhiste auditimeetodite (CAAT) kasutamine (jätkub)

4 CAAT-VAHENDITE DOKUMENTEERIMINE

4.1 Töödokumendid

4.1.1 CAAT-vahenditega sammhaaval sooritatav protsess tuleks adekvaatsete auditi asitõendite saamiseks piisavalt dokumenteerida.

4.1.2 Konkreetsemalt, auditi töödokumendid peaksid sisaldama piisavalt dokumentatsiooni CAAT-vahendite rakendamise kohta, sealhulgas üksikasju, mis on esitatud järgmistes jaotistes.

4.2 Plaanimine

4.2.1 Dokumentatsioonis tuleks hõlmata

- CAAT-vahendite eesmärgid,
- kasutamisele kuuluvad CAAT-vahendid,
- rakendatavad ohjemeetmed,
- personal ja ajastus.

4.3 Sooritamine

4.3.1 Dokumentatsioonis peaksid olema

- CAAT-vahendite ettevalmistamise ja testimise protseduurid ja ohjemeetmed;
- CAAT-vahenditega sooritatud testide üksikasjad;
- üksikasjad sisendandmete (näiteks: kasutatud andmete, failide struktuur), töötluse (näiteks CAAT-vahendite üldised vooskeemid, loogika), ja väljundandmete (näiteks: logifailid, aruanded) kohta;
- asjassepuutuvate parameetrite või lähtekoodi listing.

4.4 Auditi asitõendid

4.4.1 Dokumentatsioonis peaksid olema

- saadud väljundandmed,
- väljundandmetega sooritatud auditianalüüsi töö kirjeldus,
- auditi leiud,
- auditi järeldused,
- auditi soovitused.

4.4.2 Andmed ja failid tuleks talletada turvalises asukohas. Lisaks tuleks ajutised tundlikud andmed, mida kasutati auditi käigus, nõuetekohaselt kõrvaldada vastavalt organisatsiooni andmekäitluse protseduuridele.

5 ARUANDLUS

5.1 CAAT-vahendite kirjeldus

5.1.1 Aruandes peaks eesmärkide, käsitlusala ja metoodika osa sisaldama rakendatud CAAT-vahendite selge kirjelduse. See kirjeldus ei tohiks olla liiga üksikasjalik, kuid ta peaks andma lugejale hea ülevaate.

5.1.2 Rakendatud CAAT-vahendite kirjeldus tuleks paigutada ka aruande põhiossa, kui seal käsitletakse mingit konkreetset leidu, mis on seotud CAAT-vahendite kasutamisega.

5.1.3 Kui rakendatud CAAT-vahendite kirjeldus on seotud mitme leiuga või on liiga detailne, tuleks see aruandes lühidalt esitada eesmärkide, käsitlusala ja metoodika osas ning anda lugeja jaoks viide lisale, milles on üksikasjalikum kirjeldus.

6 JÕUSTUMISKUUPÄEV

6.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. detsembril 1998 või pärast seda. Läbivaadatud ja ajakohastatud suunis jõustub 1. märtsil 2008.

G4 IS-tegevuste tellimine teistelt organisatsioonidelt

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S1 "Audititalituse põhikiri" määrab: "Infosüsteemide auditi talituse või infosüsteemide auditi talituse eesmärk, kohustused, õigused ja vastutus peaksid olema auditi põhikirjas või töövõtukirjas selgelt dokumenteeritud."

1.1.2 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.3 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.2 Seos suunistega

1.2.1 Suunis G16 seletab, kuidas peaks IS audiitor järgima ISACA IS auditeerimise standardeid ja COBITit, kui ta hindab kolmanda poole toimet organisatsiooni IS juhtimismeetmetele ja nendega seotud juhtimiseesmärkidele.

1.3 Seos COBITiga

1.3.1 TT2 "Hallata kolmandate osapoolte teenuseid" määrab, et IS audiitor peaks välja selgitama, millised meetmed on teenuse kasutaja kehtestanud täitma ärinõuet "tagada, et kolmandate poolte rollid ja kohustused on selgelt määratletud, neid täidetakse ja nad on üha nõuetekohased".

1.4 Suunise vajadus

1.4.1 Organisatsioon (teenuse kasutaja) võib kõik oma IS-tegevused või osa neist täielikult või osaliselt delegeerida välisele selliste teenuste tarnijale (teenuseandjale). Väljasttellitavate IS-tegevuste hulka võivad kuuluda sellised IS-funktsioonid nagu arvutuskeskuse käitus, turve ning rakendussüsteemide väljatöötamine ja hooldus.

1.4.2 Lepingutele, kokkulepetele ja õigusaktidele vastavuse kinnitamine jääb teenusekasutaja hooleks.

1.4.3 Auditeerimisõigused on sageli ebaselged. Ka vastutus auditeerimise vastavuse eest ei ole sageli selge. Käesoleva juhise eesmärk on seletada, kuidas IS audiitor peaks selles olukorras järgima standardeid S1, S5 ja S6.

1.4.4 See suunis annab juhiseid IS auditeerimise standardite rakendamiseks. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardite elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

G4 IS-tegevuste tellimine teistelt organisatsioonidelt (jätkub)

2 AUDITITALITUSE PÕHIKIRI

2.1 Kohustused, õigused ja vastutus

2.1.1 Kui IS funktsiooni mingi aspekt tellitakse väliselt teenuseandjalt, tuleks need teenused võtta auditi põhikirja käsitlusalasse.

2.1.2 Auditi põhikiri peaks selgelt sõnastama IS audiitori õiguse

- vaadata läbi teenuse kasutaja ja teenuseandja vaheline lepe (enne või pärast jõustumist);
- sooritada väljasttellitava funktsiooni alal sellist audititööd, mida peetakse vajalikuks;
- teha leiud, järeldused ja soovitused teatavaks teenuse kasutaja juhtkonnale.

3 PLAANIMINE

3.1 Faktiotsing

3.1.1 IS audiitor peaks saama ettekujutuse väljasttellitavate teenuste iseloomust, ajastusest ja ulatusest.

3.1.2 Tuleks tuvastada ja kaalutleda väljasttellitavate teenustega seotud riskid.

3.1.3 IS audiitor peaks kaalutlema, millises ulatuses annavad teenuse kasutaja juhtimismeetmed mõistliku kinnituse sellele, et talitluseesmärgid saavutatakse ning et soovimatud sündmused välditakse või et nad tuvastatakse ja korrigeeritakse.

3.1.4 IS audiitor peaks endale selgeks tegema, milliseid meetmeid on kohustatud rakendama teenuseandja (või täiendavad allettevõtjaist kolmandad pooled) ja milliseid teenuse kasutaja.

3.1.5 IS audiitor peaks välja selgitama, millises ulatuses sätestab väljasttellimise lepe teenuseandja auditeerimist, ja kaaluma, kas see säte on adekvaatne. Seejuures tuleb hinnata võimalikku sõltuvust IS audititööst, mida sooritavad teenuseandja sisemised audiitorid või sõltumatu kolmas pool, kellega teenuseandja on sõlminud lepingu.

3.2 Plaanimine

3.2.1 Lepingu ja teenusetasemeleppe (SLA) läbivaatamisel plaanimisjärgus, eesmärgiga selgitada välja õigus auditeerida teenuseandjat, selle ulatus ja võimalikud seda puudutavad sätted, peaks IS audiitor kaaluma õigusabi saamist sobivalt asjatundjalt.

G4 IS-tegevuste tellimine teistelt organisatsioonidelt (jätkub)

3.2.2 IS audiitor peaks hindama kõiki teenuseandja jaoks varem koostatud auditiaruandeid ning plaanima infosüsteemide auditi töö taotlema auditi eesmärke, mis on asjakohased teenuseandja keskkonnas, võttes arvesse plaanimise ajal hangitud teabe.

3.2.3 IS audiitor peaks mõtlema sellele, millist tüüpi väljasttellimist on kasutatud ja kuidas see mõjutab auditi metoodikat.

- Tööjõu väljasttellimine (levinud välismaalt tellimise mudel).

  - Väljast tellitakse ainult tööjõud. Teenuse kasutaja sisemised meetmed ja äriprotsessid jäävad samaks. Teenuseandja sõltub teenuse andmiseks täielikult teenuse kasutaja IT-keskkonnast.

  - IS audiitor peaks plaanima teenusekasutaja seniste IT-meetmete kontrollimise ja ka kõigi teenusetasemelepet toetavate lisameetmete kontrollimise.

- Tööjõu ja süsteemide väljasttellimine (levinud asukohamaalt tellimise mudel).

  - Teenuseandja kasutab teenuse andmiseks omaenda IT-keskkonda (näiteks palgaarvestuse väljasttellimisel).

  - IS audiitor peaks mõtlema sellele, kas teenuseandja võib esitada mingit dokumentatsiooni meetmete kontrollimise kohta, mille sooritas kvalifitseeritud sõltumatu kolmas pool (näiteks SAS70 aruanne, tüüp II), ning kas kontrollimisega kaetud eesmärgid on kohaldatavad IS audiitori auditieesmärkidele.

3.2.4 Auditi eesmärgid tuleks enne teenuseandjale teatamist leppida kokku teenuse kasutaja juhtkonnaga. Kõik teenuseandja taotletavad muudatused tuleks leppida kokku teenuse kasutaja juhtkonnaga.

3.2.5 Töö käsitlusala ja eesmärkide otsustamisel peaks IS audiitor arvestama väljasttellimisele kohaldatavaid rahvusvahelisi sertifitseeringuid või raamstruktuure ja Rahvusvahelise Standardiorganisatsiooni nõudeid. Selle põhjal peaks IS audiitor otsustama, mil määral saab toetuda teenuseorganisatsiooni rahvusvahelistele sertifitseeringutele.

3.2.6 IS audiitor peaks plaanima infosüsteemide auditi töö nii, et see vastaks kohaldatavatele kutsealastele auditi standarditele, ja nii, nagu sooritataks audit teenuse kasutaja enda keskkonnas.

4 AUDITITÖÖ SOORITAMINE

4.1 Auditi asitõendite nõue

4.1.1 Audit tuleks sooritada nii, nagu antaks teenust selle kasutaja enda IS keskkonnas.

G4 IS-tegevuste tellimine teistelt organisatsioonidelt (jätkub)

4.2 Kokkulepe teenuseandjaga

4.2.1 IS audiitor peaks arvestama järgnevat:

- teenuseandja ja teenuse kasutaja vahelise formaalse leppe olemasolu;
- väljasttellimise leppe klauslit, mis selgelt määrab, et teenuseandja on kohustatud täitma kõiki ta tegevustele kohaldatavaid õigusnorme ning järgima kõiki õigusakte, mis puudutavad neid funktsioone, mida ta hakkab täitma teenuse kasutaja eest;
- väljasttellimise leppe konkreetseid ja kohustuslikke sätteid selle kohta, et teenuseandja sooritatavad tegevused allutatakse juhtimismeetmetele ja audititele nii, nagu sooritaks neid tegevusi teenuse kasutaja ise;
- teenuse kasutaja siseauditi personali ja teenuse kasutaja auditeerimisi sooritavaid kolmandaid pooli hõlmavat auditi pääsuõiguste määramist teenuseandjaga sõlmitud leppes;
- leppe sätteid, mis nõuavad, et teenuseandja seiraks vastavust teenusetasemelepetele (SLA) ja aegsasti teataks kõigist intsidentidest või meetmete tõrgetest;
- soorituse seire protseduure sisaldavate teenusetasemelepete olemasolu;
- teenuse kasutaja turvapoliitikate järgimist;
- teenuseandja usalduskindlustuse korralduse adekvaatsust;
- teenuseandja personalipoliitikate ja -protseduuride adekvaatsust, sealhulgas kohustuste lahusust olulistes tööülesannetes;
- täiendavatelt kolmandatelt pooltelt allettevõtuna teenuste tellimist ja nende teenuseandjate SLA-le vastavuse seiret käsitlevate teenuseandja poliitikate ja protseduuride adekvaatsust;
- teenuseandja jätkusuutlikkuse adekvaatsust hädaolukorras.

4.3 Väljasttellitavate teenuste haldus

4.3.1 IS audiitor peaks kontrollima, kas

- teenusetasemelepete järgimise seireks kasutatavat teavet andvaid äriprotsesse juhitakse asjakohaselt. Teenuse kasutaja peaks olema leppinud teenuseandjalt saadava tüüpse teenusetasemele vastavuse teabega või lisanud täiendavaid aruandlusnõudeid, millega teenuseandja on nõustunud;
- teenuse kasutaja on teenusetasemeleppe rikkumise korral püüdnud midagi ette võtta ja on kaalunud parandusmeetmeid kokkulepitud teenusetaseme saavutamiseks;
- teenuse kasutaja on suuteline ja pädev saadavaid teenuseid jälgima ja läbi vaatama.

G4 IS-tegevuste tellimine teistelt organisatsioonidelt (jätkub)

4.4 Käsitlusala kitsendused

4.4.1 Kui ilmneb, et teenuseandja ei taha teha koostööd IS audiitoriga, peaks audiitor sellest teatama teenuse kasutaja juhtkonnale. See võib hõlmata ka tegevusi, mis teenuseandja on allettevõtuna tellinud täiendavatelt kolmandatelt pooltelt, lülitamata lepingusse auditeerimisõiguse sätet.

5 ARUANDLUS

5.1 Aruande esitamine ja kooskõlastamine

5.1.1 Auditi töö lõpetamisel peaks IS audiitor esitama teenuse kasutaja poolsetele ettemääratud adressaatidele sobivas vormis aruande.

5.1.2 Enne aruande esitamist peaks IS audiitor mõtlema aruande läbiarutamisele teenuseandjaga, kuid audiitor ei ole kohustatud esitama lõplikku aruannet teenuseandjale. Kui teenuseandja peab ühe eksemplari saama, peaks ta selle tavaliselt saama teenuse kasutaja juhtkonnalt.

5.1.3 Aruandesse tuleks märkida kõik levitamise kitsendused, mida IS audiitor või teenuse kasutaja juhtkond soovib rakendada. Näiteks ei tohiks teenuseandja ilma IS audiitori organisatsiooni loata (ja asjakohastel juhtudel ilma teenuse kasutaja loata) anda ühtki aruande eksemplari oma teenuse teistele kasutajatele. IS audiitor peaks kaaluma ka sellise sätte lisamist, mis välistab kohustused kolmandate poolte ees.

5.2 Käsitlusala kitsendused

5.2.1 Kui auditi juurdepääsuõigusi ei tunnustatud, peaks auditi aruanne selgelt piiritlema käsitlusala kitsenduse ning seletama, milline on sellise kitsenduse mõju auditile.

6 JÄRELTEGEVUSED

6.1 Eelmiste auditite mõju

6.1.1 Nii nagu auditi sooritamisel teenuse kasutaja enda keskkonnas, peaks IS audiitor taotlema eelmiste asjassepuutuvate leidude, järelduste ja soovituste kohta asjakohast teavet nii teenuse kasutajalt kui ka teenuseandjalt. IS audiitor peaks välja selgitama, kas teenuseandja on aegsasti rakendanud sobivaid parandusmeetmeid.

7 JÕUSTUMISKUUPÄEV

7.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. septembril 1999 või pärast seda. Läbivaadatud ja ajakohastatud suunis jõustub 1. mail 2008.

G5 Audititalituse põhikiri

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S1 "Audititalituse põhikiri" määrab: "Infosüsteemide auditi talituse või infosüsteemide auditi ülesande täitja eesmärk, kohustused, õigused ja vastutus peaksid olema auditi põhikirjas või töövõtukirjas selgelt dokumenteeritud."

1.2 Seos COBITiga

1.2.1 SM 4.7 "Sõltumatu kinnitus" määrab: "... Anda juhatusele õigeaegne sõltumatu kinnitus selle kohta, et IT vastab ta poliitikatele, standarditele ja protseduuridele ning üldtunnustatud tavadele."

1.2.2 SM 2.5 "Sisejuhtimise kinnitus" määrab: "Vajadusel saada sisejuhtimismeetmete täielikkuse ja toimivuse kohta lisakinnitus kolmandate poolte sooritatud läbivaatustega."

1.3 Suunise vajadus

1.3.1 Käesoleva suunise eesmärk on aidata IS audiitoril koostada audititalituse põhikiri, millega määratleda IS auditi talituse kohustused, õigused ja vastutus. See suunis on määratud eelkõige sisemisele IS auditi talitusele, kuid ta aspekte võib arvestada ka muudes olukordades.

1.3.2 See suunis annab juhiseid IS auditeerimise standardite rakendamise kohta. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardi elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

2 AUDITITALITUSE PÕHIKIRI

2.1 Mandaat

2.1.1 IS audiitoril peaks olema selge mandaat IS auditi ülesannete täitmiseks. Harilikult dokumenteeritakse see mandaat audititalituse põhikirjas, mis tuleks formaalselt kinnitada. Kui põhikiri on kehtestatud kogu audititalituse jaoks, tuleks sellesse võimaluse korral alati võtta IS auditi mandaat.

2.2 Audititalituse põhikirja sisu

2.2.1 Audititalituse põhikiri peaks selgelt käsitlema nelja aspekti: eesmärki, kohustusi, õigusi ja vastutust. Aspektid, mida tuleb arvestada, on esitatud järgmistes alajaotistes.

G5 Audititalituse põhikiri (jätkub)

2.2.2 Eesmärk:

- roll,
- sihid,
- missiooni määrang,
- käsitlusala,
- kitsamad eesmärgid.

2.2.3 Kohustused:

- tegutsemispõhimõtted,
- sõltumatus,
- seos välise auditiga,
- auditeeritava nõuded,
- kriitilised edutegurid,
- kesksed soorituse indikaatorid,
- riski kaalutlemine,
- muud soorituse mõõdud.

2.2.4 Õigused

- õigus juurdepääsuks auditite sooritamisse puutuvale teabele, isikutele, kohtadele ja süsteemidele,
- käsitlusala või kõik selle kitsendused,
- auditeerimisele kuuluvad talitlusalad,
- auditeeritava ootused,
- organisatsiooniline struktuur, sealhulgas alluvus nõukogule ja kõrgemale juhtkonnale,
- IS auditeerimise personali ametiastmed.

2.2.5 Vastutus

- alluvus kõrgemale juhtkonnale,
- ülesannete täitmise hindamised,
- personali soorituse hindamised,
- ametikohtade ja ametialase edenemise arendus,
- auditeeritavate õigused,
- sõltumatud kvaliteediläbivaatused,
- standarditele vastavuse hindamine,
- soorituse ja tööülesannete mõõtlus,

- auditiplaani täitmise hindamine,
- eelarveliste ja tegelike kulude võrdlus,
- kokkulepitud meetmed (näiteks sanktsioonid) juhtudeks, kus üks pooltest ei täida oma kohustusi.

2.3 Suhtlus auditeeritavatega

2.3.1 Suhtlus auditeeritavatega on toimiv, kui sellega hõlmatakse

- teenuse, ta käsitlusala, ta käideldavuse ja tarnimise õigeaegsuse kirjeldamine;
- kulude hinnangud või eelarved, kui need on olemas;
- probleemide ja nende võimalike lahenduste kirjeldamine;
- adekvaatsete ja kergesti kättesaadavate vahendite andmine toimivaks suhtluseks;
- pakutava teenuse ja auditeeritava vajaduste vahelise seose määramine.

2.3.2 Audititalituse põhikiri kujutab endast mõistlikku alust suhtluseks auditeeritavatega ning peaks sisaldama viiteid teenusetasemelepetele sellistes küsimustes nagu

- kättesaadavus plaaniväliseks tööks,
- aruannete väljastus,
- kulud,
- reageerimine auditeeritava kaebustele,
- teenuse kvaliteet
- soorituse läbivaatus,
- suhtlus auditeeritavatega,
- vajaduste hindamine,
- juhtimisriski isehindamine,
- auditite pädevuse kokkuleppimine,
- aruandluse protsess,
- kokkulepe leidude kohta.

G5 Audititalituse põhikiri (jätkub)

2.4 Kvaliteedi tagamise protsess

2.4.1 IS audiitor peaks mõtlema kvaliteedi tagamise protsessi loomisele IS auditi talituse jaoks asjakohaste auditeeritava vajaduste ja ootuste mõistmiseks (näiteks: küsitlused, kliendi rahulolu uuringud, ülesande täitmise uuringud jne). Neid vajadusi tuleks hinnata põhikirjaga võrreldes, teenuse täiustamise eesmärgil või teenuse tarnimise või audititalituse põhikirja muutmiseks vastavalt vajadusele.

3 TÖÖVÕTUKIRI

3.1 Eesmärk

3.1.1 Töövõtukirju kasutatakse sageli individuaalsete ülesannete puhul või välise IS audititalituse ja organisatsiooni vahelise suhte käsitlusala ja eesmärkide seadmiseks.

3.2 Sisu

3.2.1 Töövõtukiri peaks selgelt käsitlema kolme aspekti: kohustusi, õigusi ja vastutust. Aspektid, mida tuleb arvestada, on esitatud järgmistes alajaotistes.

3.2.2 Kohustused:

- käsitlusala,
- eesmärgid,
- sõltumatus,
- riski kaalutlemine,
- auditeeritava erinõuded,
- väljastatavad tulemid.

3.2.3 Õigused:

- õigus juurdepääsuks ülesande täitmisse puutuvale teabele, isikutele, kohtadele ja süsteemidele,
- käsitlusala või kõik selle kitsendused,
- kokkulepe tõendus ülesande täitmise pädevuse kohta.

3.2.4 Vastutus

- aruannete ettemääratud adressaadid,
- auditeeritavate õigused,
- kvaliteediläbivaatused,
- kokkulepitud lõpetamiskuupäevad,
- kokkulepitud eelarved või tasud (kui on).

G5 Audititalituse põhikiri (jätkub)

4 JÕUSTUMISKUUPÄEV

4.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. septembril 1999 või pärast seda. Läbivaadatud ja ajakohastatud suunis jõustub 1. veebruaril 2008.

G6 Kaalukuse kontseptsioonid infosüsteemide auditeerimisel

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.2 Standard S10 "IT ohje" määrab: " IS audiitor peaks kontrollima ja hindama vastavust õiguslikele, keskkonna ja teabe kvaliteedi alastele ning usaldatavus- ja turvanõuetele."

1.1.3 Standard S12 "Kaalukus auditis" määrab: "Auditiprotseduuride iseloomu, ajastuse ja ulatuse määramisel peaks IS audiitor arvestama kaalukust auditis ja kaalukuse seost auditi riskiga. Auditi plaanimisel peaks IS audiitor arvestama juhtimismeetmete võimalikku nõrkust või puudumist ja seda, kas niisugune juhtimise nõrkus või puudumine võiks tekitada infosüsteemis olulise puuduse või kaaluka nõrkuse. IS audiitor peaks arvestama kumulatiivset toimet, mis võib väikesed juhtimise puudused ja nõrkused ning meetmete puudumise muundada oluliseks puuduseks või kaalukaks nõrkuseks infosüsteemis.

1.1.4 Standard S9 "Korratused ja ebaseaduslikud toimingud" määrab:

Kui IS audiitor tuvastab kaaluka korratuse või ebaseadusliku toimingu, millesse on segatud juhtkond või töötajad, kellel on oluline roll sisejuhtimises, või saab teavet kaaluka korratuse või ebaseadusliku toimingu võimaliku asetleidmise kohta, peaks ta selle aegsasti teatavaks tegema asjakohasele juhtkonna tasemele.

1.2 Seos COBITiga

1.2.1 PO5 "Hallata IT-investeeringuid" määrab: "IT-le esitatavat kuluefektiivsuse pideva ja tõendatava kasvu ning äritegevuse kasumlikkusesse lõppkasutaja ootustele vastavate integreeritud ja standardsete teenustega panuse andmise ärinõuet rahuldav IT-investeeringute haldamise IT-protsessi juhtimine saavutatakse keskendumisega toimivatele ja tõhusatele otsustustele IT-investeerimise ja -portfelli kohta ning IT-eelarvete joondamisega IT-strateegiat ja -investeeringuid puudutavate otsuste järgi ja nende eelarvete jälgimisega."

1.2.2 HE1 "Tuvastada automatiseeritud lahendused" rahuldab tegevusalast nõuet IT-le – muundada ettevõtte talitluslikud ja juhtimisnõuded automatiseeritud lahenduste toimivaks ja tõhusaks kavandiks – keskendumisega tehniliselt teostatavate ja kuluefektiivsete lahenduste leidmisele.

1.2.3 TT10 "Hallata probleeme" rahuldab tegevusalast nõuet IT-le – tagada lõppkasutajate rahulolu teenusepakkumuste ja teenusetasemetega, vähendades lahenduse ja teenusetarne defekte ja ümbertegemist – keskendumisega käitusprobleemide jäädvustamisele, jälitusele ja lahendamisele, kõigi oluliste probleemide algpõhjuse uurimisega ning tuvastatud käitusprobleemidele lahenduste määratlemisega.

G6 Kaalukuse kontseptsioonid infosüsteemide auditeerimisel (jätkub)

1.2.4 TT13 "Hallata käitust" rahuldab tegevusalast nõuet IT-le – säilitada andmeterviklus ning tagada, et IT infrastruktuur suudab vastu panna vigadele ja tõrgetele ning taastuda neist – keskendumisega plaanilise andmetöötluse käituslike teenusetasemete tagamisele, tundlike väljundandmete kaitsele ning infrastruktuuri seirele ja hooldusele.

1.2.5 SH4 "Tagada IT haldus" rahuldab tegevusalast nõuet IT-le – liita IT haldus üleorganisatsioonilise halduse eesmärkidega, järgides õigusnorme – keskendumisega juhatusele aruannete koostamisele IT strateegia, töönäitajate ja riskide kohta ning reageerimisele haldusnõuetele kooskõlas juhtkonna suunistega.

1.2.6 Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ning arvestades COBITi teabekriteeriume ja nendega seotud juhtimistavasid. Et IS audiitor saaks järgida infosüsteemide auditeerimisel kaalukuse kontseptsiooni, on COBITist valitud ja sobitatud tõenäoliselt kõige asjakohasemad protsessid ning need on alljärgnevas liigitatud esma- ja teisejärgulisteks. Valitavad ja sobitatavad protsessid ja juhtimiseesmärgid võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest.

1.2.7 Teisejärgulised

- PO8 – Hallata kvaliteeti
- PO9 – Hinnata IT riskid ja hallata neid
- HE2 – Hankida rakendustarkvara ja hooldada seda
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE4 – Võimaldada käitus ja kasutamine
- HE5 – Hankida IT-ressursid
- HE6 – Hallata muutusi
- TT3 – Hallata suutlikkust ja võimsust
- TT5 – Tagada süsteemide turvalisus
- TT9 – Hallata konfiguratsiooni
- SH1 – Seirata ja hinnata IT töötulemusi
- SH2 – Seirata ja hinnata sisejuhtimist

1.2.8 Auditikaalukuse seisukohalt kõige asjassepuutuvamad teabekriteeriumid on

- esmajärjekorras: konfidentsiaalsus, terviklus, vastavus, usaldatavus;
- teises järjekorras: toimivus, tõhusus, käideldavus.

G6 Kaalukuse kontseptsioonid infosüsteemide auditeerimisel (jätkub)

2 SUUNISE VAJADUS

2.1 IS audit ja rahandusaudit

2.1.1 IS audiitorid vajavad kaalukuse mõõtmiseks teistsuguseid mõõdupuid kui rahandusaudiitorid. Rahandusaudiitorid mõõdavad harilikult kaalukust rahalises väljenduses, sest seda, mida nad auditeerivad, mõõdetakse ja teatatakse samuti rahalises väljenduses. IS audiitorid võivad auditeerida mitterahalisi objekte, näiteks füüsilise pääsu reguleerimise meetmeid, loogilise pääsu reguleerimise meetmeid ning personalihalduse, tootmise juhtimise, kvaliteedikujunduse, paroolide genereerimise, krediitkaartide valmistuse ja patsientide hoolduse süsteeme. IS audiitorid vajavad seetõttu võib-olla juhiseid selle kohta, kuidas tuleks hinnata kaalukust, nii et nad saaksid plaanida oma auditid toimivalt, kuidas tuleks keskendada oma pingutused suure riskiga aladele ning kuidas hinnata kõigi leitud vigade või nõrkuste kaalukust.

2.1.2 See suunis annab juhiseid IS auditeerimise standardite rakendamise kohta auditikaalukusele. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardite elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

3 PLAANIMINE

3.1 Kaalukuse hindamine

3.1.1 Otsustada, mis on kaalukas, on kutsealase otsustusvõime küsimus, kus tuleb arvestada auditeeritaval alal juhtimise nõrkuste tõttu tekkida võivate vigade, tegematajätmiste, korratuste ja ebaseaduslike toimingute mõju ja/või potentsiaalset mõju organisatsiooni võimele saavutada oma ärieesmärke.

3.1.2 Kaalukuse hindamisel tuleks IS audiitoril võtta arvesse

- juhtkonnale, IS audiitorile, asjakohastele reguleerivatele asutustele ja muudele huvipooltele vastuvõetav agregeeritud veatase;
- võimalus, et väikeste vigade või nõrkuste kumulatiivne toime võib muutuda kaalukaks.

3.1.3 Auditi eesmärkide saavutamiseks peaks IS audiitor välja selgitama asjassepuutuvad juhtimiseesmärgid ja otsustama riskitaluvuse määra põhjal, mida tuleks uurida. Konkreetse juhtimiseesmärgi seisukohalt on kaalukas meede selline meede või meetmerühm, milleta ei anna juhtimisprotseduurid mõistlikku kinnitust sellele, et see juhtimiseesmärk saavutatakse.

3.1.4 Kui IS auditi eesmärk on seotud süsteemide või operatsioonidega, mis töötlevad rahalisi tehinguid, tuleks IS auditi läbiviimisel arvestada rahandusaudiitori kaalukusemõõtu.

G6 Kaalukuse kontseptsioonid infosüsteemide auditeerimisel (jätkub)

3.1.5 IS audiitor peaks kindlaks tegema rollide ja kohustuste kehtestamise, infovarade liigituse nende konfidentsiaalsuse, käideldavuse ja tervikluse järgi, pääsu reguleerimise reeglid õiguste haldamisel ning teabe liigituse ta elutähtsuse astme ja ohustatuse riski järgi. Hindamine peaks sisaldama alljärgneva kontrollimist:

- talletatav teave,
- IS riistvara,
- IS arhitektuur ja tarkvara,
- IS võrgu infrastruktuur,
- IS käitus,
- arendus- ja testimiskeskkond.

3.1.6 IS audiitor peaks kindlaks tegema, kas mõni IT üldine puudus võiks potentsiaalselt muutuda kaalukaks. Selliste puudulike IT üldiste meetmete olulisust tuleks hinnata seoses nende toimega rakenduste meetmetele, st teha kindlaks, kas nendega seotud rakenduste meetmed on samuti toimetud. Kui rakenduse puuduse põhjustab üldine IT-meede, on selle meetme puudus kaalukas. Kui näiteks rakendusel põhinev maksuarvutus on kaalukalt väär ja selle põhjuseks on halvad maksutabelite muutmise meetmed, on rakenduspõhine meede (arvutus) ja üldine meede (muudatused) kaalukalt nõrgad.

3.1.7 IS audiitor peaks hindama IT üldise meetme puudulikkust seoses ta toimega rakenduste meetmetele ja agregeerituna muude meetmete puudustega. Näiteks juhtkonna otsus mitte kõrvaldada mingit IT üldise meetme puudust ja sellega seotud mõju juhtimiskeskkonnale võib agregeerituna muude juhtimiskeskkonda mõjutavate meetmepuudustega muutuda kaalukaks.

3.1.8 IS audiitor peaks ka pidama silmas, et mingi puuduse kõrvaldamata jätmine võib muutuda kaalikaks.

3.1.9 IS audiitor peaks mõtlema kinnituse saamist asjakohastelt huvipooltelt organisatsioonis, kes tõendavad, et nad on avastatud kaalukast puudusest teadlikud.

3.1.10 Järgnevas on näiteid mõõtudest, millele tuleks mõelda kaalukuse hindamisel:

- süsteemi või operatsioonidega toetatavate talitlusprotsesside elutähtsus;
- süsteemi või operatsioonidega toetatavate teabe andmebaaside elutähtsus;
- väljatöötatavate rakenduste arv ja tüüp;
- infosüsteemide kasutajate arv;
- privileegidega liigitatud infosüsteeme kasutavate juhtide arv;
- süsteemi või operatsioonidega toetatava võrgusuhtluse elutähtsus;
- süsteemi või operatsiooni maksumus (riistvara, tarkvara, personal, kolmandate teenused, üldkulud või kõigi nende kombinatsioon);

G6 Kaalukuse kontseptsioonid infosüsteemide auditeerimisel (jätkub)

- võimalik vigade hind (tõenäoliselt väljendatult kaotatud müügina, garantiitaotlustena, tasuvuseta arenduskuludena, hoiatustest tulenevad üldsussuhete kulud, paranduskulud, tervishoiu- ja ohutuskulud, tarbetult suured tootmiskulud, suured kaod jne);
- elutähtsa ja olulise teabe kaotamise kulud teabe taastamiseks kuluva raha ja aja kujul;
- vastumeetmete toimivus;
- perioodi kestel töödeldavate pöörduste, tehingute või päringute arv;
- koostatavate aruannete ja säilitatavate failide iseloom, ajastus ja maht;
- käideldavate materjalide iseloom ja kogused (näiteks kui materjalide liikumine registreeritakse ilma rahaliste väärtusteta);
- teenusetasemeleppe nõuded ja võimalike sanktsioonide hind;
- sanktsioonid õigusaktide ja lepingute nõuete rikkumise eest;
- sanktsioonid tervishoiu- ja tööohutusnõuete nõuete rikkumise eest.

3.1.11 Juhtimise tõrgete tagajärgedeks võivad olla rahaline kahju, konkurentsipositsiooni halvenemine, usalduse või maine kaotus, organisatsiooni imago kahjustus. IS audiitor peaks hindama riske võimalike vastumeetmetega võrreldes.

4 ARUANDLUS

4.1 Aruandesse kuuluva määramine

4.1.1 Aruandesse kuuluvate leidude, järelduste ja soovituste otsustamisel peaks IS audiitor kaaluma kõigi leitud vigade kaalukust ning ka juhtimise nõrkustest tuleneda võivate vigade potentsiaalset kaalukust.

4.1.2 Kui juhtkond kasutab auditit kinnituse saamiseks IS juhtimismeetmete kohta, tähendaks meetmete adekvaatsust nentiv täpsustamata arvamus, et rakendatud meetmed vastavad juhtimiseesmärkide saavutamiseks üldtunnustatud juhtimistavadele ning kaalukaid juhtimise nõrkusi ei ole.

4.1.3 Juhtimise nõrkus tuleks lugeda kaalukaks ja seega aruandesse kuuluvaks, kui juhtimismeetme puudumise tulemusena ei saa anda mõistlikku kinnitust sellele, et juhtimiseesmärk saavutatakse. Kui audititöö tuvastab kaalukaid juhtimise nõrkusi, peaks IS audiitor kaaluma täpsustatud või negatiivse arvamuse avaldamist auditi eesmärgi kohta.

4.1.4 Sõltuvalt auditi eesmärkidest peaks IS audiitor kaaluma juhtkonna teavitamist nõrkustest, mis ei ole kaalukad, eriti kui juhtimismeetmete tugevdamise kulud on väikesed.

G6 Kaalukuse kontseptsioonid infosüsteemide auditeerimisel (jätkub)

5 JÕUSTUMISKUUPÄEV

5.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. septembril 1999 või pärast seda. Läbivaadatud ja ajakohastatud suunis jõustub 1. mail 2008.

G7 Kutsealane hoolikus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S3 "Kutse-eetika ja standardid" määrab: "IS audiitor peaks auditiülesannete täitmisel järgima ISACA kutse-eetika koodeksit."

1.1.2 Standard S3 "Kutse-eetika ja standardid" määrab: " Auditiülesannete täitmisel peaks IS audiitor ilmutama vajalikku kutsealast hoolikust, sealhulgas järgima kohaldatavaid kutsealaseid auditeerimise standardeid."

1.1.3 Standard S2 "Sõltumatus" määrab: "Kõigis auditiga seotud küsimustes peaks IS audiitor olema auditeeritavast sõltumatu nii oma hoiakult kui ka esinemiselt."

1.1.4 Standard S4 "Kutsealane pädevus" määrab: "IS audiitor peaks olema kutsealaselt pädev, tal peaksid olema auditiülesande täitmiseks vajalikud oskused ja teadmised. IS audiitor peaks oma kutsealast pädevust ülal hoidma asjakohase pideva kutsealase õppe ja koolitusega."

1.1.5 Lisajuhiseid annavad IS audiitorile ülalnimetatud standardite kommentaariosad.

1.2 Seos COBITiga

1.2.1 PO6 "Teavitada juhtimissihid ja -suund" rahuldab IT-le esitatavat ärinõuet – anda täpset ja õigeaegset teavet praeguste ja tulevaste IT-teenuste ning nendega seotud riskide ja kohustuste kohta – keskendumisega täpsete, arusaadavate ja heakskiidetud poliitikate, protseduuride, suuniste ja muu dokumentatsiooni andmisele IT juhtimise raamstruktuuri kuuluvatele huvipooltele.
1.2.2 PO7 "Hallata IT inimressursse" rahuldab IT-le esitatavat ärinõuet – IT-teenuseid peavad looma ja väljastama pädevad ja motiveeritud inimesed – keskendumisega töötajate palkamisele ja koolitamisele, motiveerimisele selgete teenistuskäikudega, oskustele vastavate rollide määramisele, määratletud läbivaatusprotsessi kehtestamisele, ametijuhendite loomisele ning isikutele toetumisest teadlikkuse tagamisele.
1.2.3 PO9 "Hinnata IT riskid ja hallata neid" rahuldab IT-le esitatavat ärinõuet – analüüsida ja teha teatavaks IT riskid ja nende võimalik toime äriprotsessidele ja -sihtidele – keskendumisega äririski ja tegutsemisriski halduse raamstruktuuridega liidetud riskihalduse raamstruktuurile, riski kaalutlemisele, riski leevendamisele ja jääkriski teatavakstegemisele.

1.2.4 SH3 "Tagada vastavus välisnõuetele" rahuldab IT-le esitatavat ärinõuet – tagada vastavus õigusaktide ja lepingute nõuetele – keskendumisega kõigi kohaldatavate õigusaktide ja lepingute väljaselgitamisele ning IT vastavuse asjakohasele tasemele ja IT-protsesside optimeerimisele lahknevusriski vähendamiseks.

1.2.5 SH4 "Tagada IT haldus" rahuldab IT-le esitatavat ärinõuet – liita IT haldus organisatsiooni halduse eesmärkidega ning järgida õigusakte ja lepinguid – keskendumisega aruannete koostamisele juhatusele IT strateegia, tulemuste ja riskide kohta ning reageerimisega haldusnõuetele kooskõlas juhatuse suunistega.

G7 Kutsealane hoolikus (jätkub)

1.2.6 Teisejärgulised viited

- PO1 – Määratleda strateegiline IT plaan
- PO5 – Hallata IT-investeeringuid
- PO8 – Hallata kvaliteeti
- PO10 – Hallata projekte
- HE1 – Tuvastada automatiseeritud lahendused
- HE6 – Hallata muutusi
- TT3 – Hallata suutlikkust ja võimsust
- TT7 – Koolitada kasutajaid
- TT9 – Hallata konfiguratsiooni
- TT10 – Hallata probleeme

1.2.7 Kõige asjssepuutuvamad teabekriteeriumid on

- esmajärjekorras: usaldatavus, konfidentsiaalsus, terviklus, vastavus ja tõhusus;
- teises järjekorras: toimivus ja käideldavus.

1.3 Suunise vajadus

1.3.1 Selle suunise eesmärk on selgitada väljendit "vajalik kutsealane hoolikus" selles tähenduses, milles teda kohaldatakse auditi sooritamisele vastavalt IS auditeerimise standardile S3.

1.3.2 ISACA liikmetelt ja sertifitseerituilt eeldatakse ISACA kutse-eetika koodeksi järgimist; koodeksi rikkumise tulemuseks võib olla liikme või sertifitseeritu käitumise uurimine ja vajadusel distsiplinaarsed sanktsioonid.

1.3.3 See suunis annab juhiseid IS auditeerimise standardite rakendamise ning ISACA kutse-eetika koodeksi järgimise kohta ülesannete täitmisel vajaliku ettevaatuse ja kutsealase hoolikusega. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardite elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

2 AUDITITÖÖ SOORITAMINE

2.1 Vajalik kutsealane hoolikus

2.1.1 Vajaliku hoolikuse norm on selline hoolikuse tase, mida mingites konkreetsetes tingimustes rakendab pädev ja mõistlik inimene. Vajalik kutsealane hoolikus kehtib sellise inimese puhul, kelle kutsealane töö praktiseerib mingit erioskust, näiteks infosüsteemide auditeerimist. Vajalik kutsealane hoolikus nõuab, et isik rakendaks seda oskust selle eriala praktiseerijatele üldiselt omasel tasemel.

G7 Kutsealane hoolikus (jätkub)

2.1.2 Vajalik kutsealane hoolikus kehtib sooritatavas töös kutsealase otsustusvõime rakendamise kohta. Vajalik kutsealane hoolikus eeldab, et professionaal käsitleb kutsealast otsustusvõimet nõudvaid küsimusi asjakohase hoolikusega. Vaatamata vajaliku kutsealase hoolikuse ja kutsealase otsustusvõime rakendamisele võib ikkagi tulla ette olukordi, kus võidakse kasutadaolevate faktide ja asjaolude hoolika läbivaatuse põhjal teha väär järeldus. Niisiis, kui tagantjärele avastatakse väär järeldus, ei tähenda see veel iseenesest IS audiitori puudulikku kutsealast otsustusvõimet või hoolikuse puudumist.

2.1.3 Vajalik kutsealane hoolikus peaks hõlmama auditi kõiki aspekte, sealhulgas auditi riski hindamist, auditiülesannete vastuvõtmist, auditi eesmärkide sõnastamist, auditi käsitlusala määramist, auditi plaanimist, auditi läbiviimist, ressursside eraldamist auditile. auditeerimistestide valimist, testimistulemite hindamist, auditi dokumenteerimist, auditi kokkuvõtete tegemist, aruandlust ja auditi tulemuste väljastust. Seejuures tuleks audiitoril määrata või hinnata

- auditi eesmärkide saavutamiseks vajalike auditiressursside tüüp, tase, oskused ja pädevus;
- tuvastatud riskide olulisus ja nende võimalik mõju auditile;
- kogutud auditi asitõendid;
- nende inimeste pädevus, korralikkus ja järeldused, kelle tööle toetub IS audiitor.

2.1.4 IS audiitor peaks kõigis IT auditiülesande täitmisega seotud küsimustes säilitama sõltumatu ja objektiivse hoiaku. Audiitor peaks auditiküsimuste käsitlemisel ja järelduste tegemisel esinema ausalt, erapooletult ja eelarvamusteta.

2.1.5 IS audiitor peaks viima auditi läbi hoolikalt, järgides kutseala standardeid ning õigusnorme ja eeskirju. IS audiitor peaks mõistlikult eeldama, et IS auditeerimise ülesande saab täita vastavalt kehtivatele IS auditeerimise standarditele ja muudele asjakohastele kutsealastele, regulatiivsetele või erialastele standarditele ning et täitmise tulemusena saab IS audit väljendada kutsealase arvamuse. Lahknevuse kõigi juhtude asjaolud peaks IS audiitor avaldama auditi tulemustest teatamisega kooskõlas oleval viisil.

2.1.6 IS audiitor peaks saama rahuldava kinnituse sellele, et juhtkond teab oma kohustusi ja vastutust auditiülesande täitmiseks vajaliku sobiva, asjassepuutuva ja õigeaegse teabe andmisel ning tagab asjassepuutuva personali koostöö auditi ajal.

2.1.7 IS audiitor peaks teenima huvipoolte huve seaduslikult ja ausalt, järgides kõrgeid käitumis- ja hoiakunorme ega tohiks panna toime elukutset diskrediteerivaid tegusid.

2.1.8 IS audiitor peaks säilitama oma ülesannete täitmise käigus saadud teabe privaatsuse ja konfidentsiaalsuse, välja arvatud juhul, kui teabe avaldamist nõuavad ametivõimud. Sellist teavet ei tohiks kasutada isiklikes huvides ega väljastada asjakohatutele pooltele.

2.1.9 Asjakohaste poolte teavitamisel töö tulemustest peaks IS audiitor ilmutama vajalikku kutsealast hoolikust.

G7 Kutsealane hoolikus (jätkub)

2.1.10 Auditi aruannete eeldatavail adressaatidel on asjakohased ootused selle kohta, et IS audiitor on kogu auditi käigus ilmutanud vajalikku kutsealast hoolikust. IS audiitor ei tohiks ülesannet vastu võtta, kui tema käsutuses ei ole adekvaatseid oskusi, teadmisi ja muid ressursse, mis on vajalikud töö lõpuleviimiseks nii, nagu seda oodatakse professionaalilt.

3 JÕUSTUMISKUUPÄEV

3.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. septembril 1999 või pärast seda. Läbivaadatud ja ajakohastatud suunis jõustub 1. märtsil 2008.

G8 Auditi dokumentatsioon

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S5 "Plaanimine" määrab: " IS audiitor peaks välja töötama ja dokumenteerima auditi plaani, mis loetleks auditi ajastuse ja ulatuse, eesmärgid ja vajalikud ressursid, detailiseerides auditi iseloomu ja eesmärgid."

1.1.2 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite asjakohase analüüsi ja tõlgendamisega. Auditiprotsess tuleks dokumenteerida, kirjeldades sooritatud auditööd ja auditi asitõendeid, mis toetavad IS audiitori leide ja järeldusi."

1.1.3 Standard S7 "Aruandlus" määrab: "Pärast auditi lõpuleviimist peaks IS audiitor koostama sobivas vormis aruande. Auditi aruanne peaks teatama sooritatud audititöö käsitlusala, eesmärgid, hõlmatud perioodi, ajastuse ja ulatuse. Aruanne peaks teatama leiud, järeldused ja soovitused ning kahtlused, piirangud või käsitlusala kitsendused, mis IS audiitoril võivad olla auditi suhtes. Väljastamisel tuleks IS audiitori aruanne varustada allkirja ja kuupäevaga ning levitada vastavalt auditi põhikirja või töövõtukirja tingimustele "

1.1.4 Standard S12 "Kaalukus auditis" määrab: " IS audiitori aruanne peaks näitama toimetuid meetmeid või meetmete puudumist ning meetmete puuduste olulisust ja nõrkuste võimalikkust, mis võivad viia olulise puuduseni või kaaluka nõrkuseni."

1.1.5 Standard S13 " Teiste spetsialistide töö kasutamine" määrab: "IS audiitor peaks määrama ja otsustama, kas teiste spetsialistide töö on adekvaatne ja täielik ning võimaldab IS audiitoril teha järelduse käsiloleva auditi eesmärkide kohta. selline järeldus tuleks selgelt dokumenteerida."

1.2 Seos COBITiga

1.2.1 PO1 "Määratleda strateegiline IT plaan" rahuldab IT-le esitatavat ärinõuet – säilitada äristrateegia ja halduse nõuded või laiendada neid, olles läbipaistev tulude, kulude ja riskide suhtes – keskendumisega IT ja talitluse halduse lülitamisele ärinõuete muundamisse teenusepakkumusteks ning strateegiate väljatöötamisele nende teenuste läbipaistvaks ja toimivaks tarnimiseks."

1.2.2 PO8 "Hallata kvaliteeti" rahuldab IT-le esitatavat ärinõuet – pidevalt ja mõõdetavalt tõsta väljastatavate IT-teenuste kvaliteeti – keskendumisega kvaliteedihalduse süsteemi määratlemisele, tulemuste pidevale seirele ettemääratud eesmärkide põhjal ning IT-teenuste pideva täiustamise kava elluviimisele.

1.2.3 HE6 "Hallata muutusi" rahuldab IT-le esitatavat ärinõuet – reageerida ärinõuetele kooskõlas äristrateegiaga, vähendades lahenduse ja teenusetarnimise defekte ja ümbertegemist – keskendumisega toime hindamise ohjele, IT infrastruktuuri, rakenduste ja tehniliste lahenduste kõigi muudatuste volitamisele ja teostamisele, puudulikust taotluste spetsifikatsioonidest tingitud vigade minimeerimisele ning volitamata muudatuste teostamise peatamisele.

1.2.4 TT1 "Määratleda teenusetasemed ja hallata neid" rahuldab IT-le esitatavat ärinõuet – tagada kesksete IT-teenuste vastavus äristrateegiale" – keskendumisega teenusenõuete väljaselgitamisele, teenusetasemete kokkuleppimisele ning teenusetasemete saavutamise seirele.

1.2.5 SH2 "Seirata ja hinnata sisejuhtimist" rahuldab IT-le esitatavat ärinõuet – kaitsta IT eesmärkide saavutamist ja järgida IT-ga seotud õigusakte – keskendudes selleks IT-ga seotud tegevuste sisejuhtimise protsesside seirele ja täiustusmeetmete piiritlemisele.

1.2.6 SH3 "Tagada vastavus välisnõuetele" rahuldab IT-le esitatavat ärinõuet – järgida õigusnorme – keskendumisega kõigi kohaldatavate õigusaktide ja sellekohaste IT vastavuse tasemete väljaselgitamisele ning IT-protsesside optimeerimisele lahknevuste riski vähendamiseks.

1.2.7 Kõige asjassepuutuvamad teabekriteeriumid on

- esmajärjekorras: usaldatavus, käideldavus, tõhusus ja terviklus;
- teises järjekorras: toimivus ja konfidentsiaalsus.

1.3 Suunise vajadus

1.3.1 Selle suunise eesmärk on kirjeldada dokumentatsiooni, mida IS audiitor peaks auditi toetuseks koostama ja säilitama.

1.3.2 See suunis annab juhiseid IS auditeerimise standardite rakendamise kohta. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardi elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

2 PLAANIMINE JA SOORITAMINE

2.1 Dokumentatsiooni sisu

2.1.1 Infosüsteemide auditi dokumentatsioon on andmik sooritatud audititöö kohta ning IS audiitori leide, järeldusi ja soovitusi toetavate auditi asitõendite kohta. Auditi dokumentatsioon peaks olema täielik, selge, struktureeritud, indekseeritud ning läbivaatajale hõlpsasti kasutatav ja arusaadav. Dokumentatsiooni võimalikud kasutusotstarbed on muuhulgas järgmised:

- tõendada, millises ulatuses on IS audiitor järginud IS auditeerimise standardeid;
- tõendada, et auditi sooritamine vastas audititalituse põhikirja nõuetele;
- abistada auditite plaanimisel, sooritamisel ja läbivaatusel;
- aidata kaasa kolmandapoolsetele läbivaatustele;
- hinnata IS auditeerimise talituse kvaliteedi tagamise kava;

G8 Auditi dokumentatsioon (jätkub)

- anda tuge sellistel juhtudel nagu kindlustusalased taotlused, pettusejuhtumid, vaidlustused ja kohtuasjad;
- abistada personali kutsealasel arendamisel.

2.1.2 Dokumentatsioon peaks jäädvustama vähemalt järgneva:

- eelmiste auditite dokumentatsiooni läbivaatuse;
- auditi käsitlusala ja eesmärkide plaanimise ja ettevalmistuse. IS audiitorid peaksid tundma läbivaadatavat valdkonda, tegevusala, äriprotsessi, toodet, tarnija tuge ja üldist keskkonda;
- juhtkondliku läbivaatuse koosolekute, auditikomisjoni koosolekute ja muude auditiga seotud koosolekute protokollid;
- auditi eesmärkidele vastava auditi kava ja auditi protseduuristiku;
- meetmete tugevate ja nõrkade külgede hindamiseks sooritatud auditisammud ja kogutud auditi asitõendid;
- auditi leiud, järeldused ja soovitused;
- audititöö tulemina väljastatud aruande;
- järelevalvelise läbivaatuse.

2.1.3 IS audiitori dokumentatsiooni ulatus sõltub konkreetse auditi vajadustest ning hõlmata tuleks näiteks järgnev:

- IS audiitori arusaam auditeeritavast alast ja selle keskkonnast;
- IS audiitori arusaam infotöötlussüsteemidest ja sisejuhtimise keskkonnast, sisaldab järgmised aspektid

  - juhtimiskeskkond,

  - juhtimisprotseduurid,

  - avastamisriski kaalutlus,

  - juhtimisriski kaalutlus,

  - ekvivalentne kogurisk.
- auditi dokumentatsiooni koostaja ja allikas ning koostamise lõpetamise kuupäev;
- meetodid, mida kasutati juhtimise adekvaatsuse hindamiseks, meetmete nõrkuse või puudumise tuvastuseks ja korvavate meetmete leidmiseks;
- auditi asitõendid, auditi dokumentatsiooni allikas ja lõpetamise kuupäev ning

  - vastavustestid, mis põhinevad testimispoliitikatel, protseduuridel ja kohustuste lahususel;

  - sõltumatud testid, mis põhinevad analüütilistel protseduuridel, detailsetel tasakaaluarvestustel ja muudel sõltumatutel auditiprotseduuridel;
- asjakohaselt isikult kinnituse saamine auditiaruande ja leidude vastuvõtmise kohta;

G8 Auditi dokumentatsioon (jätkub)

- auditeeritava reageerimine soovitustele.
- versioonihaldus, eriti kui dokumentatsioon on elektroonilisel kandjal.

2.1.4 Dokumentatsioon peaks sisaldama sobivat audititeavet, mida nõuavad seadused, valitsuse määrused või kohaldatavad kutseala standardid.

2.1.5 Dokumentatsioon tuleks esitada auditikomisjonile läbivaatamiseks ja kinnitamiseks.

3 DOKUMENTATSIOON

3.1 Dokumentatsiooni hoidmine, säilitus ja kasutamine

3.1.1 Auditi leide ja järeldusi toetava dokumentatsiooni asjakohase hoidmise ja säilituse tagamiseks õiguslike, kutsealaste ja organisatsiooniliste nõuete täitmiseks piisava aja kestel peaksid olema kehtestatud poliitikad ja protseduurid.

3.1.2 Dokumentatsioon tuleks korraldada, ladustada ja turvata tema säilitamiseks kasutatava infokandja jaoks sobival viisil ning ta peaks olema kasutamiseks kättesaadav ülalmääratletud poliitikate ja protseduuride rahuldamiseks piisava aja kestel.

4 JÕUSTUMISKUUPÄEV

4.1 Läbivaatusele võetud suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. septembril 1999 või pärast seda. Läbivaadatud ja ajakohastatud suunis jõustub 1. märtsil 2008.

G9 Korratuste arvestamine auditeerimisel

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S3 "Kutse-eetika ja standardid" määrab: "Auditiülesannete täitmisel peaks IS audiitor ilmutama vajalikku kutsealast hoolikust, sealhulgas järgima kohaldatavaid kutsealaseid auditeerimise standardeid."

1.1.2 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.3 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.4 Standard S7 "Aruandlus" määrab: "Pärast auditi lõpuleviimist peaks IS audiitor koostama sobivas vormis aruande. Aruandesse tuleks märkida organisatsioon, eeldatavad saajad ja võimalikud levituskitsendused. Auditi aruanne peaks teatama sooritatud auditi töö käsitlusala, eesmärgid, hõlmatud perioodi, ajastuse ja ulatuse. Aruanne peaks teatama leiud, järeldused ja soovitused ning kahtlused, piirangud või käsitlusala kitsendused, mis IS audiitoril võivad olla auditi suhtes.

1.1.5 Standard S9 „Korratused ja ebaseaduslikud toimingud“ täpsustab nõudeid ja IS audiitori kaalutlusi, mis puudutavad korratusi ja ebaseaduslikke toiminguid.

1.2 Suunise vajadus

1.2.1 Mõningaid korratusi võib lugeda petutoiminguteks. Petutoiminguteks määramine sõltub pettuse õiguslikust määratlusest konkreetset auditit hõlmavas jurisdiktsioonis. Korratuste hulka kuuluvad lisaks muudele sihilik turvameetmetest möödahiilimine kavatsusega varjata pettuse, lubamatu varade või teenuste kasutamise jms jätkumist ning sedalaadi toimingute varjamise toetamine või abistamine. Pettuseta korratuste hulka võivad kuuluda

- kehtiva halduspoliitika sihilikud rikkumised,
- eeskirjade nõuete sihilikud rikkumised,
- auditeeritavat ala või kogu organisatsiooni puudutavad sihilikud väärütlused või teabe väljajätud,
- üldine silmatorkav lohakus,
- ettekavatsematud ebaseaduslikud toimingud.

1.2.2 See suunis annab juhiseid IS auditeerimise standardite rakendamise kohta. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardi elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

G9 Korratuste arvestamine auditeerimisel (jätkub)

2 AUDITITALITUSE PÕHIKIRI

2.1 Kohustused

2.1.1 IS audiitor peaks mõtlema sellele, et määratleda audititalituse põhikirjas või töövõtukirjas juhtkonna ja auditi kohustused korratuste vältimise, avastamise ja neist teatamise osas, nii et need kohustused oleksid selgesti arusaadavad kogu audititöös. Kui need kohustused on juba dokumenteeritud organisatsiooni pettusetõrje poliitikas või muus sellises dokumendis, tuleks see märkida audititalituse põhikirja.

2.1.2 Juhtkond vastutab pettuse vältimist ja avastamist sisaldavate sisemiste meetmete kavandamise, teostamise ja käigushoiu eest.

2.1.3 IS audiitori kohustus on kaalutleda pettuse risk ning kavandada ja sooritada kontrollimisi, mis sobivad auditiülesande iseloomuga ning mille rakendamisel võib mõistlikult eeldada, et nad avastavad

- korratusi, millel võib olla kaalukas mõju auditeeritavale alale või organisatsioonile tervikuna;
- sisemeetmete nõrkusi, mis võivad tuleneda vältimata või avastamata jäänud kaalukatest korratustest.

2.1.4 Audit ei saa garanteerida korratuste avastamist. Ka siis, kui audit plaanitakse ja sooritatakse asjakohaselt, võivad korratused jääda avastamata, näiteks, kui töötajate vahel on salakokkulepe, kui töötajate ja väliste poolte vahel on salakokkulepe või kui korratustesse on segatud juhtkond. IS audiitor peaks mõtlema ka selle asjaolu dokumenteerimisele auditalituse põhikirjas või töövõtukirjas.

3 PÄDEVUS

3.1 Pettuseteadlikkus

3.1.1 IS audiitor peaks mõõdukalt valdama pettuse teemat, nii et ta suudaks tuvastada riskitegureid, mis võivad aidata kaasa pettuse asetleidmisele.

4 PLAANIMINE

4.1 Riski kaalutlemine

4.1.1 IS audiitor peaks kaalutlema auditeeritava alaga seotud korratuste ilmnemise riski. Selle kaalutluse koostamisel tuleks tal arvesse võtta muuhulgas sellised tegurid:

- organisatsiooni iseloom, näiteks üleorganisatsioonilist eetika, organisatsiooni struktuur, järelevalve-, korvamis- ja hüvitusstruktuuride adekvaatsus, tulemuslikkussurve ulatus;
- organisatsiooni ajalugu;

G9 Korratuste arvestamine auditeerimisel (jätkub)

- hiljutisi juhtimise, tegutsemise või infosüsteemide muudatusi;
- hoitavate varade või pakutavate teenuste liigid ja nende tundlikkus korratuste suhtes;
- asjassepuutuvate meetmete tugevus;
- kohaldatavad eeskirjade või õigusaktide nõuded;
- eelmiste auditite leidude ajalugu;
- organisatsiooni tegevusala ja tegutsemise konkurentsikeskkond;
- väljaspool auditi käsitlusala sooritatud läbivaatuste leiud, näiteks konsultantide, kvaliteedi tagamise töörühmade või juhtkonna spetsiifiliste uuringute leiud;
- igapäevase töö käigus ilmnenud leiud;
- auditeeritavat ala toetava(te) infosüsteemi(de) tehniline arengutase ja keerukus;
- oma jõududega väljatöötatud või enda hooldatavate rakendussüsteemide olemasolu kesksete talitlussüsteemide tarbeks, võrreldes tarkvarapakettidega.

4.1.2 Auditiülesande iseloomuga sobivaaudititöö plaanimisel peaks IS audiitor riski kaalutlemise tulemite põhjal otsustama sellise kontrolli iseloomu, ajastuse ja ulatuse, mis on vajalik piisavate auditi asitõendite saamiseks, mis annavad mõistliku kinnituse sellele, et

- tuvastatakse korratused, millel võib olla kaalukas mõju auditeeritavale alale või organisatsioonile tervikuna;
- tuvastatakse selliste meetmete nõrkused, millega ei õnnestu vältida või avastada kaalukaid korratusi.

5 AUDITITÖÖ SOORITAMINE

5.1 Korratuste leidmise mõju

5.1.1 Korratuste avastamisel peaks IS audiitor hindama nende toimingute mõju auditi eesmärkidele ja kogutud asitõendite usaldatavusele. Peale selle peaks IS audiitor kaaluma, kas jätkata auditit, kui

- korratuste mõju osutub nii oluliseks, et piisavaid usaldusväärseid auditi asitõendeid ei saa hankida;
- auditi asitõenditest järeldub, et juhtkond on korratustes osalenud või neid mahitanud.

G9 Korratuste arvestamine auditeerimisel (jätkub)

5.2 Korratusemärkide leidmise mõju

5.2.1 Kui auditi asitõendid näitavad, et võisid aset leida korratused, peaks IS audiitor

- soovitama juhtkonnal asja detailselt uurida või rakendada asjakohaseid meetmeid. Kui IS audiitoril on kahtlus, et juhtkond osaleb korratuses, peaks ta organisatsioonis välja selgitama asjakohase vastutava töötaja, kellele ta peaks need järeldused teatavaks tegema. Kui sisemine teatamine osutub võimatuks, peaks IS audiitor kaaluma konsulteerimist auditikomisjoni ja juristiga, leidudest väljapoole organisatsiooni teatamise soovitatavuse ja riskide küsimuses;
- sooritama adekvaatsed toimingud auditi leidude, järelduste ja soovituste toetuseks.

5.3 Õigusalased kaalutlused

5.3.1 Kui auditi asitõendid näitavad, et mingi korratusega võis kaasneda ebaseaduslik tegu, Peaks IS audiitor kaaluma otsest õigusalast konsulteerimist või soovitama juhtkonnal otsida õigusabi.

6 ARUANDLUS

6.1 Sisemine aruandlus

6.1.1 Korratuste avastamisest tuleks organisatsioonis õigel ajal teatada asjakohastele isikutele. Teade tuleks suunata kõrgemale juhtkonna tasemele kui see, kus arvatavasti leidsid aset korratused. Peale selle tuleks korratustest teatada juhatusele, juhatuse auditikomisjonile või sellele vastavale organile, välja arvatud asjades, mis on nii rahalise mõju poolest kui ka juhtimise nõrkuste märgina selgesti tähtsusetud.

6.1.2 Hoolikalt tuleks kaaluda korratuseteadete sisemist levitamist. Korratuste asetleidmine ja mõju on tundlik küsimus ja neist teatamisega kaasnevad oma riskid, sealhulgas

- juhtimismeetmete nõrkuste edasine kuritarvitamine nõrkuste üksikasjade avaldamise tulemusena;
- klientide, tarnijate ja investeerijate kaotamine, kui nõrkused paljastatakse (volitatult või volitamatult) väljaspool organisatsiooni;
- oluliste töötajate ja juhtide (sealhulgas nende, kes polnud segatud korratusse) kaotus, kui väheneb usk juhtkonda ja organisatsiooni tulevikku.

6.1.3 IS audiitor peaks mõtlema sellele, et teatada korratusesteraldi, lahus muudest auditi küsimustest, kui see aitab reguleerida aruande levitamist.

G9 Korratuste arvestamine auditeerimisel (jätkub)

6.2 Väline aruandlus

6.2.1 Välist aruandlust võivad kohustada õigusaktid või eeskirjad. See kohustus võib kehtida organisatsiooni juhtkonna kohta või korratuse avastamises osalenute kohta või mõlema kohta.

6.2.2 Kui nõutakse välist aruandlust, peaks aruande enne ta avaldamist väljaspool kinnitama asjakohane auditi juhtkonna tase ning auditeeritava juhtkond peaks selle eelnevalt läbi vaatama, kui seda ei välista kohaldatavad eeskirjad või auditi konkreetsed tingimused. Näiteid konkreetsetest tingimustest, mis võivad välistada nõusoleku hankimise auditeeritava juhtkonnalt:

- auditeeritava juhtkond on aktiivselt segatud korratusse;
- auditeeritava juhtkond mahitab passiivselt korratust.

6.2.3 Kui auditeeritava juhtkond ei nõustu aruande avaldamisega väljaspool, kuid välist aruandlust kohustavad põhikiri või õigusaktid, peaks IS audiitor kaaluma konsulteerimist auditikomisjoni ja juristiga, leidudest väljapoole organisatsiooni teatamise soovitatavuse ja riskide küsimuses.

6.2.4 Auditi juhtkonna nõusolekul peaks IS audiitor õigel ajal esitama aruande kõigile asjakohastele organitele.

6.2.5 Kui IS audiitor teab, et juhtkond on kohustatud pettusetoimingutest aru andma mingile välisele organisatsioonile, peaks ta juhtkonnale ametlikult soovitama seda kohustust täita.

6.2.6 Kui korratuse avastas IS audiitor, kes ei kuulu välisauditi töörühma, peaks ta kaaluma õigeaegset aruande esitamist välisaudiitoritele.

6.3 Auditi käsitlusala kitsendused

6.3.1 Auditi käsitlusala kitsendamise korral peaks IS audiitor kirjeldama auditi aruandes sellise kitsenduse iseloomu ja mõju. Niisugune kitsendus võib leida aset, kui

- IS audiitor ei saanud teha osa tööst, mis oli vajalik auditi algsete eesmärkide saavutamiseks ja auditi järelduste toetuseks – näiteks ebausaldatavate auditi asitõendite, ressursside puudumise või auditi tegevuste juhtkonnapoolsete kitsenduste tõttu;
- juhtkond ei ole sooritanud IS audiitori soovitatud uurimisi.

7 JÕUSTUMISKUUPÄEV

7.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. märtsil 2000 või pärast seda.

G10 Valimkontroll auditeerimisel

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite asjakohase analüüsi ja tõlgendamisega."

1.2 Suunise vajadus

1.2.1 Selle suunise eesmärk on anda IS audiitorile juhiseid auditivalimi kavandamiseks ja valimiseks ning valimkontrolli tulemuste hindamiseks. Sobiv valimivõtt ja hindamine täidab nõuded "piisavad, usaldusväärsed ja asjassepuutuvad asitõendid" ning "toetada asjakohase analüüsiga".

1.2.2 IS audiitor peaks mõtlema valimismeetoditele, mis annavad vastavuse või olulisuse kontrollimiseks statistiliselt representatiivse valimi.

1.2.3 Näiteid meetmetest, mille vastavuse kontrollimisel võib kaaluda valimi kasutamist: kasutaja pääsuõigused, programmide muutmise ohje protseduurid, protseduuride dokumenteerimine, erindite järeltoimingud, logide läbivaatus, tarkvaralitsentside revisjonid jms.

1.2.4 Näiteid olulisuse kontrollimistest, kus võib kaaluda valimi kasutamist: keerulise arvutuse (näiteks intressiarvutuse) ülearvutamine kontode valimiga, tehingute abidokumentatsiooni kontrollimine tehingute valimiga jms.

1.2.5 See suunis annab juhiseid IS auditeerimise standardite rakendamise kohta. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardi elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

1.2.6 Valimkontrolli kohta auditeerimisel annab kasulikku alusmaterjali muuhulgas Rahvusvahelise Raamatupidamisföderatsiooni (IFAC) väljaantud Auditeerimise rahvusvaheline standard nr. 530 "Valimkontroll ja muud valikulise kontrolli protseduurid".

2 AUDITITÖÖ SOORITAMINE

2.1 Valimkontroll auditeerimisel

2.1.1 Piisavate, usaldatavate ja asjassepuutuvate auditi asitõendite saamiseks peaks IS audiitor statistiliste või mittestatistiliste valimivõtu meetodite abil kavandama ja valima auditeerimisvalimi, sooritama auditi protseduurid ja hindama valimkontrolli tulemusi.

G10 Valimkontroll auditeerimisel (jätkub)

2.1.2 Auditi arvamuse kujundamisel ei uuri IS audiitorid tihti kogu nende käsutuses olevat teavet, sest see võib olla ebapraktiline, õigete järeldusteni võib aga jõuda valimkontrolli abil.

2.1.3 Auditi valimkontroll määratletakse kui auditiprotseduuride rakendamine vähemale kui 100 protsendile üldkogumist, nii et IS audiitoril oleks võimalik hinnata auditi asitõendeid valitud objektide mingi omaduse järgi ja et see kujundaks või aitaks kujundada järeldust kogu üldkogumi kohta.

2.1.4 Statistilise valimkontrolliga kaasneb selliste meetodite kasutamine, millega saab üldkogumi kohta teha matemaatiliselt tuletatud järeldusi.

2.1.5 Mittestatistiline valimkontroll ei põhine statistikal ning tulemeid ei tohi ekstrapoleerida üldkogumile, sest tõenäoliselt ei ole valim üldkogumi suhtes representatiivne.

2.2 Valimi kavandamine

2.2.1 Auditivalimi suuruse ja struktuuri kavandamisel peaksid IS audiitorid arvestama konkreetseid auditi eesmärke, üldkogumi iseloomu ning valimite moodustamise ja valimise meetodeid.

2.2.2 IS audiitor peaks kaaluma vajadust kaasata valimite kavandamisse ja analüüsimisse asjakohaseid spetsialiste.

2.2.3 Valimiüksus. Valimiüksus sõltub valimi otstarbest. Meetmete vastavuse kontrollimiseks kasutatakse tavaliselt atribuutide valimkontrolli, kus valimiüksuseks on sündmus või tehing (meede võib olla näiteks lubav kinnitus arvetel). Olulisuse kontrollimisel kasutatakse tihti muutujate valimkontrolli või statistiliste hinnangutega valimkontrolli, kus valimiüksus on sageli rahaline.

2.2.4 Auditi eesmärgid. IS audiitor peaks arvestama konkreetseid auditi eesmärke, mis tuleb saavutada, ja auditi protseduure, millega võib kõige tõenäolisemalt jõuda nende eesmärkideni. Kui auditi valimkontroll on sobiv, tuleks peale selle arvestada otsitavate auditi asitõendite iseloomule ja võimalikele veaolukordadele.

2.2.5 Üldkogum. Üldkogum on kogu see andmekogum, millest IS audiitor tahab võtta valimit järelduse tegemiseks üldkogumi kohta. Seetõttu peab üldkogum, millest võetakse valim, olema asjakohane ning ta täielikkus auditi konkreetse eesmärgi seisukohalt peab olema tõendatud.

2.2.6 Kihitamine. Valimi tõhusa ja toimiva kavandamise soodustamiseks võib olla kasu kihitamisest. Kihitamine on protsess, millega üldkogum jagatakse ühesuguste selgelt määratletud omadustega alamkogumiteks, nii et iga valimiüksus saab kuuluda ainult ühte kihti.

2.2.7 Valimi maht. Valimi mahu määramisel peaks IS audiitor arvestama valimiriski, aktsepteeritavat vea suurust ja oodatavate vigade ulatust.

2.2.8 Valimirisk. Valimirisk tekib võimalusest, et IS audiitori järeldused võivad erineda järeldustest, milleni jõutaks sama auditiprotseduuri rakendamisel kogu üldkogumile. Valimiriske on kahesuguseid:

- väära aktsepteerimise risk on risk pidada kaalukat vääresitust ebatõenäoliseks, sellal kui üldkogum on esitatud kaalukalt vääralt;
- väära eituse risk on risk pidada kaalukat vääresitust tõenäoliseks, sellal kui üldkogum ei ole esitatud kaalukalt vääralt.

2.2.9 Valimi mahtu mõjutab valimiriski suurus, mida IS audiitor soovib aktsepteerida. Valimiriski tuleks vaadelda ka auditi riski mudeli ja selle komponentide, olemusriski, meetmeriski ja avastamisriski seisukohalt.

2.2.10 Talutav viga. Talutav viga on üldkogumis maksimaalne viga, mida IS audiitorid nõustuvad aktsepteerima, tehes ikkagi järelduse, et auditi eesmärk on saavutatud. Olulisuse kontrollimiste puhul on talutav viga seotud IS audiitori otsusega kaalukuse kohta. Vastavuse kontrollimistel on see maksimaalne lahknevus ettekirjutatud juhtimisprotseduurist, mida IS audiitor nõustub aktsepteerima..

2.2.11 Eeldatav viga. Kui IS audiitor eeldab, et üldkogumis on vigu, tuleb järelduse tegemiseks, et tegelik viga üldkogumis ei ole suurem plaanitud talutavast veast, harilikult uurida suuremat valimit kui vigade puudumise eeldamisel. Kui eeldatakse, et üldkogumis ei ole vigu, on õigustatud väiksemad valimi mahud. Üldkogumi eeldatava vea määramisel peaks IS audiitor arvestama selliseid tegureid nagu eelmistel auditit tuvastatud vigade suurused, muudatused organisatsiooni protseduurides ning asitõendid, mis on saadud sisejuhtimise süsteemi hindamisest ja analüütiliste läbivaatuse protseduuride tulemitest.

2.3 Valimivõtt

2.3.1 Üldkasutatavaid valimivõtu meetodeid on neli.

Statistilised valimivõtu meetodid:

- juhuslik valimivõtt – tagab, et kõigil valimiüksuste kombinatsioonidel üldkogumis on ühesugune võimalus sattuda valimisse;
- süstemaatiline valimivõtt – seisneb valimiüksuste võtus mingi ettemääratud vahemiku järel, kusjuures esimese vahemiku algus on juhuslik. Näide: valimine rahaüksuste järgi ehk väärtusega kaalutud valimine, kus igal üksikul rahalisel väärtusel (näiteks $1) on üldkogumis võrdne võimalus sattuda valimisse. Harilikult ei saa küll iga rahaüksust uurida eraldi, kuid uurimiseks valitakse element, mis sisaldab seda rahaüksust. See meetod kaalub valimit süstemaatiliselt suuremate summade kasuks, kuid annab siiski igale rahalisele väärtusele võrdse võimaluse sattuda valimisse. Teine näide: iga n-nda valimiüksuse valimine.

Mittestatistilised valimivõtu meetodid

- huupi valimivõtt – IS audiitor võtab valimi, järgimata mingit struktureeritud meetodit, kuid vältides igasuguseid teadlikke nihkeid ja ettearvatusi. Huupi võetud valimi analüüsile ei saa aga toetuda järelduse tegemiseks üldkogumi kohta;

- otsuslik valimivõtt – IS audiitor võtab valimi mingi nihkega (näiteks: kõik teatud väärtust ületavad valimiüksused, kõik teatud tüüpi erandid, kõik negatiivsed, kõik uued kasutajad jne). Tuleks silmas pidada, et otsuslik valimivõtt ei põhine statistikal ning tulemusi ei tohiks ekstrapoleerida üldkogumile, sest tõenäoliselt ei ole valim üldkogumi suhtes representatiivne.

2.3.2 IS audiitor peaks võtma valimiüksused nii, et kontrollitavate omaduste seisukohalt võiks eeldada valimi representatiivsust üldkogumi suhtes, st ta peaks kasutama statistilisi valimivõtu meetodeid. Auditi sõltumatuse säilitamiseks peaks IS audiitor veenduma, et üldkogum on täielik ja ohjama valimivõttu.

2.3.3 Et valim oleks üldkogumi suhtes representatiivne, peaksid kõigil valimiüksustel üldkogumis olema võrdne või teadaolev valimisse sattumise tõenäosus, st tuleks kasutada statistilisi valimivõtu meetodeid.

2.3.4 On kaks üldkasutatavat valimismeetodit: valimine kirjetest ja valimine kvantitatiivsetelt väljadelt (näiteks rahaüksuste puhul).

Kirjetest valimise levinud meetodid on

- juhuslik valimine (statistiline valim),
- huupi valimine (mittestatistiline),
- otsuslik valimine (mittestatistiline, suur tõenäosus jõuda nihutatud järelduseni).

Kvantitatiivsetelt väljadelt valimise levinud meetodid on

- juhuslik valimine (statistiline valim rahaüksustest),
- püsivahemikuga valimine (statistiline valim püsiva vahemikuga),
- lahtervalimine (statistiline valim, juhusliku valimisega mingis vahemikus).

2.4 Dokumentatsioon

2.4.1 Auditi töödokumendid peaksid sisaldama piisavaid üksikasju valimkontrolli eesmärkide ja kasutatud valimkontrolli protsessi selgeks kirjeldamiseks. Töödokumendid peaksid näitama üldkogumi allikat, kasutatud valimivõtu meetodit, valimivõtu parameetreid (näiteks juhuslikku alustusarvu või juhusliku alustamise meetodit, valimisvahemikku), valitud objekte, sooritatud auditkontrollide üksikasju ja tehtud järeldusi.

2.5 Valimivõtu tulemite hindamine

2.5.1 Kui IS audiitor on iga valimiüksusega sooritanud konkreetse auditi eesmärgi jaoks sobivad auditiprotseduurid, peaks ta analüüsima kõiki valimis avastatud võimalikke vigu, et teha kindlaks, kas need on tegelikult vead ja võimaluse korral selgitada välja nende vigade iseloom ja põhjus. Kui kasutatud valimivõtu meetod on statistikapõhine, tuleks tegelikeks hinnatud vead vastavalt vajadusele projekteerida üldkogumile.

G10 Valimkontroll auditeerimisel (jätkub)

2.5.2 Kõik valimis avastatud võimalikud vead tuleks läbi vaadata, et teha kindlaks, kas nad on tegelikult vead. IS audiitor peaks arvestama vigade kvalitatiivseid aspekte, sealhulgas vea iseloomu ja põhjust ning vea võimalikku mõju auditi teistele järkudele. Automatiseeritud protsessi avarii tulemuseks olevatel vigadel on tavaliselt laiem mõju vigade määrale kui inimeksitustel.

2.5.3 Kui oodatavat auditi asitõendit mingi konkreetse valimiobjekti kohta ei õnnestu saada, on IS audiitoril võib-olla võimalik hankida piisavaid asjakohaseid auditi asitõendeid valitud objektile mingite alternatiivsete protseduuride rakendamise teel

2.5.4 IS audiitor peaks mõtlema valimitulemite projekteerimisele üldkogumile sellise projektsioonimeetodiga, mis oleks kooskõlas valimiüksuse võtuks kasutatud meetodiga. Valimi projekteerimine võib sisaldada tõenäolise vea hindamist üldkogumis ning kõigi meetodi ebatäpsuse tõttu avastamata jäänud vigade hindamist ja kõigi leitud vigade kvalitatiivsete aspektide hindamist.

2.5.5 IS audiitor peaks kaaluma, kas vead üldkogumis võivad ületada talutavaid vigu, võrreldes selleks projekteeritud üldkogumiviga talutava veaga ja arvestades auditi eesmärgi jaoks asjakohaseid muude auditiprotseduuride tulemeid. Kui projekteeritud üldkogumiviga ületab talutava vea, peaks IS audiitor uuesti kaalutlema valimiriski ja kui see risk ei ole aktsepteeritav, siis kaaluma auditiprotseduuri laiendamist või alternatiivsete auditiprotseduuride sooritamist.

3 JÕUSTUMISKUUPÄEV

3.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. märtsil 2000 või pärast seda.

G11 IS üldmeetmete toime

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.2 Suunise vajadus

1.2.1 Iga organisatsiooni, osakonna või talituse haldus ja seire mõjutavad seda, kuidas see organisatsioon, osakond või talitus käitub, sealhulgas seda, kuidas ta rakendab juhtimismeetmeid. See põhimõte kehtib nii IT kasutamise kohta kui ka tööstusettevõtte, krediidiosakonna või rahandustalituse kohta.

1.2.2 Organisatsioonis kasutatavate IS detailmeetmete toimivust piirab infosüsteemide kasutamise haldus ja seire kogu organisatsioonis tervikuna. Seda tunnistatakse tihti rahandusauditite juhistes, kus nenditakse "üldiste" IS keskkonna meetmete toimet "rakenduste" meetmetele rahandussüsteemides. Näiteks ütleb UK auditeerimisjuhis 3.2.407 ("Auditeerimine arvutikeskkonnas"): "Tugevad üldmeetmed lisavad audiitori võimalikku kindlustunnet rakenduse meetmete suhtes. Puudulikud üldmeetmed võivad õõnestada tugevaid rakenduse meetmeid või halvendada puudulikke rakenduse meetmeid."

1.2.3 COBIT annab raamstruktuuri, mis võib aidata IS audiitoril eristada

- detailseid IS meetmeid, mis puutuvad otseselt IS auditi käsitlusalasse;
- IS halduse ja seire funktsioone, mis lisavad audiitori võimalikku kindlustunnet nende detailsete IS meetmete suhtes.

1.2.4 Meetmete jaotus üldisteks ja rakenduste meetmeteks kavandati spetsiaalselt selliste auditite tarbeks, mille eesmärk on kujundada arvamus selle kohta, kas rahandusteabes on või ei ole kaalukaid vääresitusi (rahandusauditite).

1.2.5 Kui siseaudiitorid ja sõltumatud konsultandid sooritavad IS auditeid, on auditil harilikult teistsugune eesmärk ja käsitlusala kui rahandusauditite. Kasutuselolevad süsteemid on käsiprotsesside ja arvutipõhiste protsesside kombinatsioon ning juhtimiseesmärgid peavad olema seatud kogu protsessile, mis võib olla laiem või kitsam raamatupidamiskirjete töötlusest. Seetõttu ei tarvitse rahandusauditite jaoks kasutatav raamstruktuur sobida mõnedele IS auditite.

1.2.6 Auditeeritavate detailmeetmete toimivuse kohta arvamuse kujundamiseks peaks IS audiitor mõtlema vajadusele hinnata infosüsteemide halduse ja seire toimivust, ka siis, kui see jääb välja kokkulepitud auditi käsitlusalast. Selliste kaalutluste tulem võib ulatuda kokkulepitud käsitlusala laiendamisest kuni asjakohaselt suunitletud aruandeni.

G11 IS üldmeetmete toime (jätkub)

1.2.7 Halduse ja seire meetmete üldkogum on lai ning osa neist meetmetest ei tarvitse puudutada konkreetset auditieesmärki. Auditi riski hindamiseks ja sobiva auditeerimismetoodika määramiseks vajab IS audiitor struktureeritud meetodit, millega selgitada välja

- need halduse ja seire meetmed, mis ei puuduta auditi käsitlusala ja eesmärke;
- need halduse ja seire meetmed, mida tuleks kontrollida;
- asjassepuutuvate halduse ja seire meetmete mõju auditi arvamusele.

Selleni võib jõuda sellise meetmete raamstruktuuri abil, mis on spetsiifiline IS ja sellega seotud tehnoloogia kasutamisele ning aitab IS audiitoril keskenduda kõige peamistele auditeeritavaid infosüsteeme ja operatsioone mõjutavatele meetmetele.

1.2.8 See suunis annab juhiseid IS auditeerimise standardite rakendamise kohta. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardi elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

2 MEETMETE RAAMSTRUKTUUR

2.1 Ülevaade

2.1.1 COBIT määratleb juhtimise kui "poliitikad, protseduurid, tavad ja organisatsioonilised struktuurid, mis on mõeldud andma mõistlikku kinnitust sellele, et talitluseesmärgid saavutatakse ning et soovimatud sündmused välditakse või nad avastatakse ja heastatakse." Iga IS auditi puhul peaks IS audiitor auditi pingutuste keskendamiseks IS auditi eesmärkidesse puutuvatele riskialadele eristama neid üldisi meetmeid, mis mõjutavad kõiki infosüsteeme ja operatsioone (IS üldmeetmeid) nendest üldistest ja rakenduste meetmetest, mis töötavad spetsiifilisemal tasemel (IS detailmeetmetest). Alljärgnevas kirjeldatud meetmete raamstruktuuri eesmärk on aidata IS audiitoril saavutada sellist keskendumist.

2.1 IS üldmeetmed

2.2.1 Termin "IS üldmeetmed" on määratletud sõnastikus. Selliste meetmete näidete hulka kuuluvad IS protsesside meetmed, mis on määratletud COBITi plaanimise ja organiseerimise valdkonnas ning seire ja hindamise valdkonnas; näiteks: PO1 "Määratleda strateegiline IT plaan" ja SH1 " Seirata ja hinnata IT töötulemusi ". IS üldmeetmed on üldiste meetmete alamhulk, niisugused üldised meetmed, mis keskenduvad IS haldusele ja seirele.

2.2.2 IS üldmeetmete mõju IS audiitori tööle ei piirdu ainult rakenduste meetmete usaldatavusega rahandussüsteemides. IS üldmeetmed mõjutavad ka nende IS detailmeetmete usaldatavust, mida rakendatakse näiteks

- programmide väljatöötamisele,
- süsteemide evitamisele,

- turbehaldusele,
- varundusprotseduuridele.

2.2.3 Nõrk infosüsteemide haldus ja seire (st nõrgad IS üldmeetmed) peaks tegema IS audiitori valvsaks: võimalik on suur risk, et detailtasemel töötama määratud meetmed ei toimi.

2.3 IS detailmeetmed

2.3.1 Termin "IS detailmeetmed" on määratletud sõnastikus. Nad koosnevad rakenduste meetmetest ja sellistest üldistest meetmetest, mis ei kuulu IS üldmeetmete hulka. COBITi raamstruktuuris on IS detailmeetmed need meetmed, mida rakendatakse infosüsteemide ja -teenuste hankimisele, teostamisele, tarnimisele ja toele. Näidete hulka kuuluvad meetmed, mida rakendatakse

- tarkvarapakettide evitamisele,
- süsteemide turvaparameetritele,
- avariijärgse taaste plaanimisele,
- andmesisestuse valideerimisele,
- eranditteadete koostamisele,
- kasutajakontode blokeerimisele pärast nurjunud pääsukatseid.

Rakenduste meetmed on üks osa IS detailmeetmetest. Näiteks on andmesisestuse valideerimine nii IS detailmeede kui ka rakenduse meede. Süsteemide installeerimine ja akrediteerimine (HE5) on IS detailmeede, kuid ei ole rakenduse meede.

2.3.2 IS meetmete vahelisi seoseid näitab järgmine liigendus:

IS meetmed

→ üldised meetmed
- IS üldmeetmed
- IS detailmeetmed

rakenduste meetmed

Peale selle peaks IS audiitor arvestama IS-väliste meetmete mõju käsitlusalale ja auditi protseduuridele.

2.4 IS üld- ja detailmeetmete interaktsioon

2.4.1 COBITi raamstruktuur jaotab IS juhtimise protsessid neljaks alaks:

- plaanimine ja organiseerimine,
- hankimine ja evitamine,
- tarnimine ja tugi,
- seire ja hindamine.

G11 IS üldmeetmete toime (jätkub)

2.4.2 Meetmete toimivust hankimise ja evitamise (HE) ning tarnimise ja toe (TT) aladel mõjutab nende meetmete toimivus, mida rakendatakse plaanimise ja organiseerimise (PO) ning seire ja hindamise (SH) aladel. Kui juhtkond plaanib, organiseerib ja seirab puudulikult, ei toimi hankimisele, evitamisele ning teenuste tarnimisele ja toele rakendatavad meetmed. Seevastu aga võib tugev plaanimine, organiseerimine ja seire tuvastada ja korrigeerida neid hankimisele, evitamisele ning teenuste tarnimisele ja toele rakendatavad meetmed, mis ei toimi.

2.4.3 Näiteks mõjutab protsessile "Hankida rakendustarkvara ja hooldada seda" (COBITi protsess HE2) rakendatavaid IS detailmeetmeid selliste IS üldmeetmete adekvaatsus, mida rakendatakse muuhulgas järgmistele protsessidele:

- "Määratleda strateegiline IT plaan" (COBITi protsess PO1),
- "Hallata projekte" (COBITi protsess PO10),
- "Hallata kvaliteeti" (COBITi protsess PO8),
- " Seirata ja hinnata IT töötulemusi " (COBITi protsess SH1).

2.4.4 Rakendussüsteemi hankimise auditi käigus tuleks välja selgitada, millist mõju avaldavad IS strateegia, projektihalduse metoodika, kvaliteedihaldus ja seiremetoodika. Kui näiteks projektihaldus on puudulik, peaks IS audiitor kaaluma järgmist:

- lisatöö kavandamist kinnituse saamiseks sellele, et konkreetset auditeeritavat projekti hallatakse toimivalt;
- juhtkonna informeerimist IS üldmeetmete nõrkustest.

2.4.5 Veel üks näide. Protsessile "Tagada süsteemide turvalisus" (COBITi protsess TT5) rakendatavate IS detailmeetmete toimivust mõjutab selliste IS üldmeetmete adekvaatsus, mida rakendatakse muuhulgas järgmistele protsessidele:

"Määratleda IT protsessid, organisatsioon ja seosed" (COBITi protsess PO4),

"Teavitada juhtimissihid ja suund" (COBITi protsess PO6),

"Hinnata IT riskid ja hallata neid" (COBITi protsess PO9),

" Seirata ja hinnata IT töötulemusi " (COBITi protsess SH1).

2.4.6 Mingi süsteemi, näiteks UNIXi, Windows NT, RATCF, turvaparameetrite adekvaatsuse auditi käigus tuleks arvestada juhtkonna turvapoliitikaid (PO6), turbekohustuste jaotust (PO4), riski hindamise protseduure (PO9) ja turvapoliitikate järgimise seire protseduure (SH1). Isegi siis, kui parameetrid ei vasta IS audiitori arusaamale "parimast tavast", võib parameetreid hinnata adekvaatseteks juhtkonna tuvastatud riski ning sellise riskitaseme käsitlemist suunavate halduspoliitikate alusel. Kõik auditi täiustussoovitused peaksid sel juhul olema suunatud riskihalduse poliitikatele ning ka üksikparameetritele endile.

G11 IS üldmeetmete toime (jätkub)

PLAANIMINE

3.1 Asjassepuutuvate IS üldmeetmete käsitlusviis

3.1.1 IS auditeerimise suunis G15 (Plaanimine) määrab, et IS audiitor peaks sooritama auditeeritava funktsiooni juhtimise eelhindamise. See eelhindamine peaks sisaldama asjakohaste IS üldmeetmete väljaselgitamist ja hindamist. IS üldmeetmete kontroll võib toimuda ka sooritatava auditi mingis teises tsüklis, sest oma loomult hõlmavad nad IS kasutamise paljusid eri aspekte. Seetõttu peaks IS audiitor mõtlema, kas nende meetmete väljaselgitamiseks ja hindamiseks saaks toetuda mingile varasemale audititööle sellel alal.

3.1.2 Kui auditi töö näitab, et IS üldmeetmed on puudulikud, peaks IS audiitor arvestama selle leiu mõju auditi eesmärkide saavutamiseks kavandatud metoodikale:

- tugevad IS üldmeetmed võivad lisada IS audiitori võimalikku kindlustunnet IS detailmeetmete suhtes;
- nõrgad IS üldmeetmed võivad nõrgendada tugevaid IS detailmeetmeid või suurendada detailtaseme nõrkusi.

3.2 Piisavad auditiprotseduurid

3.2.1 Kui IS üldmeetmetel on oluline potentsiaalne mõju auditi eesmärgile, ei piisa auditi plaanimisest detailmeetmete ulatuses. Kui IS üldmeetmete auditeerimine pole võimalik või praktiline, tuleks sellisest käsitlusala kitsendusest teatada.

3.2.2 Kui see aitab saavutada auditi eesmärki, peaks IS audiitor plaanima asjassepuutuvate IS üldmeetmete kontrollimise.

3.3 Asjassepuutuvad meetmed

3.3.1 Asjassepuutuvad IS üldmeetmed on need meetmed, mis mõjutavad auditiülesande konkreetseid eesmärke. Näiteks kui auditi eesmärk on teatada meetmetest, mis puudutavad teatava programmiteegi muudatusi, puutuvad asjasse need IS üldmeetmed, mis on seotud turvapoliitikatega (PO6), kuid asjasse ei tarvitse puutuda need IS üldmeetmed, mis on seotud tehnoloogilise suuna määramisega (PO3).

3.3.2 Auditi plaanimisel peaks IS audiitor IS üldmeetmete koguhulga kohta välja selgitama, millised neist meetmeist mõjutavad konkreetseid auditi eesmärke, ning plaanima nende lülitamise auditi käsitlusalasse. Asjassepuutuvaid IS üldmeetmeid võivad IS audiitoril aidata määrata COBITi juhtimiseesmärgid "Plaanimise ja organiseerimise" ning "Seire ja hindamise" aladelt.

G11 IS üldmeetmete toime (jätkub)

3.4 Auditi asitõendid

3.4.1 IS üldmeetmed võivad olla dokumenteerimata, kuid IS audiitor peaks plaanima auditi asitõendite hankimise selle kohta, et asjassepuutuvad meetmed toimivad. Võimalikud kontrollimised on visandatud jaotises "Audititöö sooritamine".

3.5 Asjassepuutuvate IS detailmeetmete käsitlusviis

3.5.1 Kui IS audititöö näitab, et IS üldmeetmed on rahuldavad, peaks IS audiitor mõtlema IS detailmeetmete plaanilise kontrollimise lõdvendamist, sest auditi asitõendid tugevate IS üldmeetmete kohta lisavad kinnitust, mida IS audiitor võib saada IS detailmeetmete kohta.

3.5.2 Kui IS audititöö näitab, et IS üldmeetmed ei ole rahuldavad, peaks IS audiitor sooritama IS detailmeetmete piisava kontrollimise auditi asitõendite hankimiseks selle kohta, et need meetmed toimivad vaatamata asjassepuutuvate IS üldmeetmete nõrkustele.

4 AUDITITÖÖ SOORITAMINE

4.1 IS üldmeetmete kontrollimine

4.1.1 IS audiitor peaks sooritama piisava kontrollimise kinnituse saamiseks asjassepuutuvate IS üldmeetmete toimivusele auditi perioodil või mingil konkreetsel hetkel. Sobivate kontrollimisprotseduuride hulka võivad kuuluda

- vaatlus;
- tõendavad uuringud;
- asjassepuutuva dokumentatsiooni (poliitikate, standardite, koosolekuprotokollide jms) läbivaatus;
- kordussooritamine (näiteks CAAT-vahendite abil).

4.1.2 Kui asjassepuutuvate IS üldmeetmete kontrollimine näitab, et nad on rahuldavad, peaks IS audiitor jätkama nende IS detailmeetmete plaanilise kontrolliga, mis on otseselt seotud auditi eesmärgiga. Selline kontroll võib olla vähem range kui ta oleks asjassepuutuvate IS üldmeetmete mitterahuldava toime korral.

5 ARUANDLUS

5.1 IS üldmeetmete nõrkused

5.1.1 Kui IS audiitor on tuvastanud IS üldmeetmetes nõrkusi, tuleb need teha juhtkonnale teatavaks ka siis, kui selliste alade käsitlus ei ole konkreetselt võetud kokkulepitud töö käsitlusalasse.

G11 IS üldmeetmete toime (jätkub)

5.2 Käsitlusala kitsendused

5.2.1 Juhul, kui IS üldmeetmed võivad oluliselt mõjutada IS detailmeetmete toimivust, aga neid ei ole auditeeritud, peaks IS audiitor tegema oma lõpparuandes selle asjaolu juhtkonnale teatavaks, koos lausungiga selle asjaolu võimalikust mõjust auditi leidudele, järeldustele ja soovitustele. Näiteks kui IS audiitor käsitleb aruandes mingi komplektlahenduse hanget, kuid pole näinud organisatsiooni IS strateegiat, peaks ta märkima aruandesse, et IS strateegia ei olnud kättesaadav või puudus üldse. Asjakohastel juhtudel peaks IS audiitor lisaks sellele teatama selle asjaolu võimaliku mõju auditi leidudele, järeldustele ja soovitustele, näiteks nentides, et seetõttu ei ole võimalik öelda, kas komplektlahenduse hange vastab IS strateegiale ja toetab tulevasi tegevuskavasid.

6 JÕUSTUMISKUUPÄEV

6.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. märtsil 2000 või pärast seda.

G12 Organisatsiooniline seos ja sõltumatus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S2 "Sõltumatus" määrab: "Kõigis auditiga seotud küsimustes peaks IS audiitor olema auditeeritavast sõltumatu nii oma hoiakult kui ka esinemiselt."

1.1.2 Standard S2 "Sõltumatus" määrab: "IS auditi talitus peaks auditiülesande objektiivseks sooritamiseks olema sõltumatu läbivaadatavast tegevusvaldkonnast."

1.1.3 Standard S3 "Kutse-eetika ja standardid" määrab: "IS audiitor peaks auditiülesannete täitmisel järgima ISACA kutse-eetika koodeksit."

1.2 Suunise vajadus

1.2.1 Selle suunise eesmärk on täpsustada sõltumatust IS auditeerimise standardis S2 kasutatud tähenduses ning käsitleda IS audiitori hoiakut ja sõltumatust infosüsteemide auditeerimisel.

1.2.2 See suunis annab juhiseid IS auditeerimise standardite rakendamise kohta. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardite elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

2 SÕLTUMATUS

2.1 Hoiak

2.1.1 IS audiitorid peaksid kogu oma töös püüdma järgida kohaldatavaid kutse-eetika koodekseid ja auditeerimise standardeid.

2.1.2 Vastavalt COBITile peaks audititalituse põhikiri tagama, et vastav organisatsiooni juhtkond säilitab ja kehtestab audititalituse sõltumatuse, õigused ja vastutuse.

3 PLAANIMINE

3.1 Töötajad

3.1.1 IS audiitor loob palju suhteid audititegevuses osalejatega ning tal on võimalus uurida auditeeritava ala kõige varjatumaid aspekte, sageli kogu organisatsiooni. IS audiitori hoiak peaks alati sobima selle rolliga. Plaanimine peaks võtma arvesse kõik teadaolevad suhted.

G12 Organisatsiooniline seos ja sõltumatus (jätkub)

3.1.2 Kui IS audiitorite sõltumatus on puudulik, ei tohiks nad osaleda auditis. Sõltumatus on puudulik näiteks siis, kui IS audiitoritel on mingeid ootusi saada rahalist kasu või muid isiklikke hüvesid, mis võivad tuleneda sellest, et audiitorid mõjutavad auditi tulemusi. IS audiitorite sõltumatus ei ole aga tingimata puudulik siis, kui nad auditeerivad selliseid infosüsteeme, kus nad igapäevase tegevuse käigus sooritavad endi isiklikke tehinguid.

3.1.3 Auditi alustamisel võib IS audiitor kinnitada oma sõltumatust huvide vastuolu deklaratsioonile allakirjutamise teel.

3.2 Prioriteetidega auditiplaan

3.2.1 COBITi lai juhtimiseesmärk SH4 määrab: "Juhtkond peaks kindlustama sõltumatu auditi". Selle eesmärgi saavutamiseks tuleks koostada auditi plaan. See plaan peaks tagama, et turbe ja sisejuhtimise protseduuride toimivusele, tõhususele ja ökonoomsusele saadakse regulaarne ja sõltumatu kinnitus. Selles plaanis peaks juhtkond määrama sõltumatu kinnituse saamiseks prioriteedid.

4 AUDITITÖÖ SOORITAMINE

4.1 Organisatsioon

4.1.1 IS audiitor peaks olema auditeeritavast alast organisatsiooniliselt sõltumatu. Sõltumatus on puudulik, kui auditeeritav ala on IS audiitori otsese kontrolli all. IS audiitori sõltumatus võib olla puudulik ka siis, kui ta allub otse neile, kelle otsese kontrolli all on auditeeritav ala.

4.1.2 IS audiitor ja juhtkond peaksid regulaarselt hindama sõltumatust. See hindamine peaks arvestama selliseid tegureid nagu muudatused isiklikes suhetes, rahalised huvid ning varasemad tööülesanded ja -kohustused. IS audiitor peaks mõtlema juhtimise enesehindamise meetodite kasutamisele niisuguses pidevas hindamisprotsessis.

4.1.3 Sõltuvalt ülesandest võib IS audiitor küsitleda inimesi, analüüsida organisatsiooni protsesse, saada abi organisatsiooni personalilt jne. IS audiitori sõltumatu hoiak ja selle ilmutamine peaksid alati olema adekvaatsed niisuguste olukordadega toimetulemiseks. IS audiitorid peaksid olema teadlikud sellest, et sõltumatuse avaldumist võivad mõjutada nende toimingud või sidemed. IS audiitori sõltumatusest jäänud muljed võivad mõjutada IS audiitori töö aktsepteerimist.

4.1.4 Kui IS audiitoritele ilmneb, et mingit olukorda või suhet tajutakse nende sõltumatust kahjustavana, peaksid nad sellest niipea kui võimalik informeerima auditi juhtkonda.

4.2 Teabe kogumine

4.2.1 Mitmesuguste auditeeritava organisatsiooni tundmaõppimiseks vajalike asjade hulgas tuleks IS audiitoritel oma sõltumatuse säilitamiseks läbi vaadata

- sõltumatu kinnituse protsessi puudutavad organisatsiooni poliitikad ja protseduurid;
- audititalituse põhikiri, missiooni sõnastus, poliitikad, protseduurid ja standardid, eelmised aruanded ja auditi plaanid;
- organisatsiooni skeem.

4.3 Meetmete hindamine

4.3.1 IS auditi plaan peaks määratlema tegevused, mille suhtes IS audiitor peab olema sõltumatu. IS audiitori sõltumatust neist tegevustest peaks regulaarselt jälgima kõrgem juhtkond või IS auditi plaani otsustaja ja kinnitaja. See jälgimine peaks sisaldama IS audiitoritele konkreetsete ülesannete määramise protsessi hindamist veendumiseks, et see protsess tagab sõltumatuse ja piisavad oskused.

4.3.2 Alati tuleks kontrollida, kas IS audiitor järgib kehtivaid kutsealase käitumise tavasid. Paljudel juhtudel peaks see olema piisav auditi asitõendite andmiseks sõltumatuse kohta. Kui on mingeid viiteid IS audiitori sõltumatuse puudulikkuse kohta, tuleks mõelda auditi plaani läbivaatamisele.

5 ARUANDLUS

5.1 Mõju aruandlusele

5.1.1 Olukordades, kus IS audiitori sõltumatus on puudulik ja IS audiitor on endiselt seotud auditiga, tuleks IS audiitori sõltumatuse küsimust ümbritsevad faktid avaldada vastavale juhtkonnale ja esitada aruandes.

6 JÕUSTUMISKUUPÄEV

6.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. septembril 2000 või pärast seda.

G13 Riski kaalutlemise kasutamine auditi plaanimisel

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.2 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite sobiva analüüsi ja tõlgendamisega."

1.1.3 Auditeerimise suunise G15 "Plaanimine" jaotis 2.4.1 määrab: "Mõistliku kinnituse saamiseks sellele, et audititöö käigus kaetakse kaalukad aspektid adekvaatselt, tuleks sooritada riski kaalutlemine. See kaalutlemine peaks välja selgitama need kohad, kus on suhteliselt suur kaalukate probleemide risk."

1.2 Suunise vajadus

1.2.1 Auditi konkreetse eesmärgi saavutamiseks vajalik audititöö tase on IS audiitori subjektiivne otsus. Selle otsuse üks aspekte on risk jõuda auditi leidude põhjal väärale järeldusele (auditirisk). Teine aspekt on auditeeritaval alal esinevate vigade risk (vearisk). Soovitatavad tavad riski kaalutlemiseks rahandusauditite sooritamisel on rahandusaudiitorite auditeerimisstandardites piisavalt dokumenteeritud, kuid vaja on juhiseid selle kohta, kuidas rakendada selliseid meetodeid IS auditites.

1.2.2 Ka oma otsustes selle kohta, kui palju juhtimist on vaja, toetub juhtkond niisuguse riskile avatuse taseme kaalutlemisele, mida ta on valmis aktsepteerima. Näiteks võimetus mingil ajavahemikul töödelda arvutirakendusi on riskile avatus, mille võivad põhjustada ootamatud ja soovimatud sündmused (näiteks tulekahi arvutuskeskuses). Riskile avatusi saab vähendada sobivalt kavandatud meetmete rakendamisega. Harilikult põhinevad need meetmed kahjulike sündmuste toimumise tõenäosuse hindamisel ning on mõeldud selle tõenäosuse vähendamiseks. Näiteks ei hoia tulesignalisatsioon ära põlenguid, kuid on mõeldud vähendama tulekahjustuse ulatust.

1.2.3 See suunis annab juhiseid IS auditeerimise standardite rakendamise kohta. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardite elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

2 PLAANIMINE

2.1 Riski kaalutlemise metoodika valimine

2.1.1 Saadaval on palju arvutipõhiseid ja muid riski kaalutlemise metoodikaid, mille hulgast IS audiitor võib valida. Metoodikad ulatuvad lihtsatest IS audiitori otsustustel põhinevatest kolmeksliigitustest (suur, keskmine, väike) keerukate ja teadusliku ilmega arvutusteni riski arvhinde saamiseks. IS audiitor peaks mõtlema, milline keerukuse ja detailsuse tase sobib auditeeritavale organisatsioonile.

G13 Riski kaalutlemise kasutamine auditi plaanimisel (jätkub)

2.1.2 Kõik riski kaalutlemise metoodikad sõltuvad protsessi mingis punktis (näiteks mitmesugustele parameetritele kaalude määramisel) subjektiivsetest otsustustest. IS audiitor peaks välja selgitama mingi konkreetse metoodika kasutamiseks vajalikud subjektiivsed otsustused ja kaaluma, kas neid otsuseid saab teha ja sobiva täpsusega valideerida.

2.1.3 Riski kaalutlemise kõige sobivama metoodika otsustamisel peaks IS audiitor võtma arvesse järgmised aspektid.

- Kogumisele kuuluva teabe tüüp. (Mõned süsteemid kasutavad ainsa mõõduna rahalist mõju, IS auditite puhul see aga alati ei sobi.)
- Metoodika kasutamiseks vajalike tarkvara- või muude litsentside hind.
- Kui suures ulatuses on vajalik teave juba olemas.
- Lisateave, mida tuleb koguda, enne kui võib saada usaldatava tulemuse: teabe kogus ja ta kogumise hind (sealhulgas kogumisele kuluv aeg).
- Metoodika teiste kasutajate arvamused ja nende otsused selle kohta, kui hästi see metoodika aitas neil tõsta oma auditite toimivust ja tõhusust.
- Juhtkonna valmisolek aktsepteerida metoodikat vahendina, millega määrata sooritatava audititöö tüüp ja tase.

2.1.4 Ei saa loota, et ükski riski kaalutlemise metoodika sobiks kõigile olukordadele. Auditeid mõjutavad tingimused võivad ajas muutuda. IS audiitor peaks perioodiliselt uuesti hindama valitud riski kaalutlemise metoodikate sobivust.

2.2 Riski kaalutlemise kasutamine

2.2.1 Valitud riski kaalutlemise meetodeid peaks IS audiitor kasutama üldise auditiplaani koostamisel ja konkreetsete auditite plaanimisel. Riski kaalutlemisele kombineeritult muude auditi meetoditega tuleks mõelda näiteks selliste plaanimisotsuste tegemisel:

- auditiprotseduuride iseloom, ulatus ja ajastus;
- auditeerimisele kuuluvad alad või talitlusfunktsioonid;
- auditile eraldatav aeg ja ressursid.

2.2.2 Riskide koondtaseme määramiseks peaks IS audiitor võtma arvesse järgmised riskitüübid:

- olemusrisk,
- juhtimisrisk,
- avastamisrisk.

G13 Riski kaalutlemise kasutamine auditi plaanimisel (jätkub)

2.3 Olemusrisk

2.3.1 Olemusrisk on audeeritava ala veakalduvus, mis võib olla kaalukas, individuaalne või kombinatsioonis muude vigadega, eeldusel, et puuduvad sellega seotud sisemised meetmed. Näiteks on operatsioonisüsteemi turvalisusega seotud olemusrisk harilikult suur, sest andmete või programmide muutmine või isegi paljastamine operatsioonisüsteemi turvanõrkuste kaudu võib viia väära juhtimisteabeni või konkurentsivõime languseni. Seevastu on autonoomse lauaarvuti turvalisusega seotud olemusrisk harilikult väike, kui korralik analüüs tõendab, et seda arvutit ei kasutata talitluse jaoks elutähtsatel eesmärkidel.

2.3.2 Enamiku IS auditeerimisalade olemuslik risk on harilikult suur, sest vigade võimalik toime hõlmab tavaliselt mitut töösüsteemi ja paljusid kasutajaid.

2.3.3 Olemusriski kaalutlemisel peaks IS audiitor arvestama nii IS üld- kui ka detailmeetmeid. See ei kehti juhtudel, kus IS audiitori ülesanne on seotud ainult IS üldmeetmetega.

2.3.4 IS üldmeetmete puhul tuleks IS audiitoril konkreetse auditeerimisala jaoks sobival tasemel võtta arvesse järgmised aspektid:

- IS juhtkonna moraalsus, kogemused ja teadmised;
- muutused IS juhtkonnas;
- surved IS juhtkonnale, mis võivad teda kallutada teavet (näiteks suurte ettevõtte jaoks elutähtsate projektide ülekulud, häkkerite tegutsemine) varjama või vääralt esitama;
- organisatsiooni tegevuse ja süsteemide iseloom (näiteks e-kaubanduse plaanid, süsteemide keerukus, integreeritud süsteemide puudumine);
- organisatsiooni kogu tegevusvaldkonda mõjutavad tegurid (näiteks muudatused tehnoloogias, IS personali kättesaadavus);
- kolmandate poolte mõju tugevus auditeeritavate süsteemide juhtimisele (tingitud näiteks tarneahela integratsioonist, väljasttellitavatest IS protsessidest, ühisettevõtetest, klientide otsepääsust);
- eelmiste auditite leiud ja toimumisajad.

2.3.5 IS detailmeetmete puhul tuleks IS audiitoril konkreetse auditeerimisala jaoks sobival tasemel võtta arvesse järgmised aspektid:

- sellel auditeerimisalal sooritatud eelmiste auditite leiud ja toimumisajad;
- auditeeritavate süsteemide keerukus;
- vajalik käsitsi sekkumise määr;
- süsteemi kontrolli all olevate (näiteks inventari loetelu või palgalehe näol) varade avatus kaotsiminekule või omastamisele;
- aktiivsusetippude tõenäosus auditiperioodi teatud aegadel;

- toimingud väljaspool igapäevast harilikku IS-töötlust (näiteks operatsioonisüsteemi utiliitide kasutamine andmete parandamiseks);
- IS meetmete rakendamises osaleva juhtkonna ja töötajate moraalsus, kogemused ja teadmised.

2.4 Juhtimisrisk

2.4.1 Juhtimisrisk on risk, mis tuleneb sellest, et sisemine juhtimissüsteem ei väldi või ei avasta ja paranda aegsasti viga, mis võib esineda auditeeritaval alal ning võib olla kaalukas, individuaalne või kombinatsioonis teiste vigadega. Näiteks võib arvuti logide käsitsi läbivaatamisega seotud risk olla suur, sest logitava teabe suure mahu tõttu võivad tihti jääda märkamata toimingud, mida tuleks uurida. Andmete arvutipõhise valideerimisega seotud juhtimisrisk on harilikult madal, sest protsesse rakendatakse järjekindlalt.

2.4.2 IS audiitor peaks kaalutlema juhtimisriski suureks, kui asjassepuutuvaid sisemeetmeid ei ole

- tuvastatud,
- hinnatud toimivaiks,
- testitud ja tõendatud, et nad toimivad, nagu vaja.

2.5 Avastamisrisk

2.5.1 Avastamisrisk on risk, mis tuleneb sellest, et IS audiitori olulised protseduurid ei avasta viga, mis võib olla kaalukas, individuaalne või kombinatsioonis teiste vigadega. Näiteks on rakendussüsteemi turvarikete tuvastamisega seotud avastamisrisk harilikult suur, sest auditi ajal pole logisid kogu auditiperioodi kohta. Avariijärgse taaste plaanide puudumise tuvastamisega seotud avastamisrisk harilikult väike, sest nende plaanide olemasolu on lihtne kontrollida.

2.5.2 Detailtestimise vajaliku taseme määramisel tuleks IS audiitoril võtta arvesse

- olemusriski hinnang;
- pärast vastavustestimist tehtud järeldus juhtimisriski kohta.

2.5.3 Mida suurem on olemusriski ja juhtimisriski hinnang, seda rohkem peaks IS audiitor tavaliselt hankima auditi asitõendeid detailsete auditiprotseduuride sooritamisel.

G13 Riski kaalutlemise kasutamine auditi plaanimisel (jätkub)

3 AUDITITÖÖ SOORITAMINE

3.1 Dokumentatsioon

3.1.1 IS audiitor peaks mõtlema konkreetse auditi jaoks kasutatava riski kaalutlemise meetodi või metoodika dokumenteerimisele. Selles dokumentatsioonis peaksid harilikult olema

- kasutatud riski kaalutlemise metoodika kirjeldus;
- oluliste turvaaukude ja neile vastavate riskide piiritlus;
- riskid ja turvaaugud, mida audit on mõeldud käsitlema;
- IS audiitori riskihinnangu toetuseks kasutatavad auditi asitõendid.

4 JÕUSTUMISKUUPÄEV

4.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. septembril 2000 või pärast seda.

G14 Rakendussüsteemide läbivaatus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Auditi tööd sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.2 Suunise vajadus

1.2.1 Selle suunise eesmärk on kirjeldada rakendussüsteemide läbivaatuse sooritamiseks soovitatavaid tavasid.

1.2.2 Rakendussüsteemide läbivaatuse eesmärk on välja selgitada, dokumenteerida, kontrollida ja hinnata rakendusele suunatud meetmed, mis organisatsioon on evitanud asjassepuutuvate juhtimiseesmärkide saavutamiseks. Neid juhtimiseesmärke võib liigitada süsteemile ja temaga seotud andmetele suunatud juhtimiseesmärkideks.

2 PLAANIMINE

2.1 Plaanimiskaalutlusi

2.1.1 Plaanimise lahutamatu osa on IS audiitori jaoks organisatsiooni infosüsteemikeskkonna tundmine niisuguses ulatuses, mis võimaldaks tal määrata süsteemide suuruse ja keerukuse ning organisatsiooni sõltuvuse oma infosüsteemidest. IS audiitor peaks õppima tundma organisatsiooni missiooni ja tegevuseesmärke, infotehnoloogia ja infosüsteemide organisatsiooni toeks kasutamise taset ja viisi ning organisatsiooni eesmärkide ja infosüsteemidega seotud riske ja avatust riskidele. Ta peaks saama ka ettekujutuse organisatsiooni struktuurist, sealhulgas kesksete IS töötajate rollidest ja kohustustest ning vaadeldavat rakendussüsteemi sisaldava talitlusprotsessi omanikust.

2.1.2 Plaanimise esmane eesmärk on tuvastada rakendustaseme riskid. Riski suhteline suurus mõjutab vajalikku auditi asitõendite määra.

2.1.3 Süsteemi ja andmete osas kuuluvad rakendustaseme riskide hulka näiteks

- süsteemi käideldavuse riskid, mis on seotud süsteemi töövõime puudumisega;
- süsteemi turvariskid, mis on seotud volitamata juurdepääsuga süsteemidele ja või andmetele;
- süsteemi tervikluse riskid, mis on seotud andmete puuduliku, väära, mitteõigeaegse või volitamata töötlusega;
- süsteemi hooldatavuse riskid, mis on seotud võimatusega ajakohastada vajaduse korral süsteemi nii, et tagataks endiselt süsteemi käideldavus, turvalisus ja terviklus;

G14 Rakendussüsteemide läbivaatus (jätkub)

- andmeriskid, mis on seotud andmete täielikkuse, tervikluse, konfidentsiaalsuse, privaatsuse ja õigsusega.

2.1.4 Rakenduste meetmed rakendustaseme riskide käsitlemiseks võivad oma kujult olla süsteemi sisseehitatud automatiseeritud meetmed, käsitsi täidetavad meetmed või nende kombinatsioon. Näiteid: dokumentide (hanketellimuse, arve ja kaupade vastuvõtuaruande) arvutipõhine võrdlemine, arvutiga genereeritud tšeki kontrollimine ja allakirjutamine, erandiaruannete läbivaatus kõrgemas juhtkonnas.

2.1.5 Juhul kui on otsustatud toetuda programmeeritud meetmetele, tuleks mõelda asjassepuutuvatele üldistele IT meetmetele ning spetsiifiliselt auditi eesmärki puudutavatele meetmetele. Üldisi IT meetmeid võiks käsitleda eraldi läbivaatusega, mis hõlmaks füüsilisi turvameetmeid, süsteemitaseme turvet, võrguhaldust, andmevarundust ja ootamatuste käsitluse plaanimist. Läbivaatuse käsitlusala sõltub läbivaatuse eesmärkidest ning IS audiitoril ei ole alati vaja vaadata läbi üldisi meetmeid, näiteks siis, kui rakendussüsteemi hinnatakse ta hankimiseks.

2.1.6 Rakendussüsteemi läbivaatusi võib sooritada siis, kui komplektset rakendussüsteemi hinnatakse ta hankimiseks, enne rakendussüsteemi käikuandmist (evituseelne läbivaatus) või pärast rakendussüsteemi käikuandmist (teostusjärgne läbivaatus). Rakendussüsteemi evituseelne läbivaatus hõlmab rakendustaseme turbe arhitektuuri, turbe evituse plaane, süsteemi ja kasutajadokumentatsiooni adekvaatsust ning tegeliku või kavandatud kasutajapoolse omaksvõtu testimise adekvaatsust. Rakendussüsteemi teostusjärgne läbivaatus hõlmab rakendustaseme turvalisust pärast evitust ja võib hõlmata süsteemi konversiooni, kui on toimunud andmete ja põhifailiteabe üleviimine vanast süsteemist uude.

2.1.7 Rakendussüsteemide läbivaatuse eesmärgid ja käsitlusala moodustavad harilikult lähtetingimuste ühe osa. Lähtetingimuste vorm ja sisu võivad varieeruda, kuid selles dokumendis peavad olema järgmised andmed:

- läbivaatuse eesmärgid ja käsitlusala;
- läbivaatust sooritav(ad) IS audiitor(id);
- lausung IS audiitori(te) sõltumatuse kohta projekti suhtes;
- läbivaatuse alustamise aeg;
- läbivaatuse kestus;
- aruandluse korraldus;
- sulgemisnõupidamise korraldus;

Eesmärgid tuleks välja töötada nii, et nad taotleksid COBITi seitsme teabekriteeriumi rahuldamist, ja seejärel organisatsioonis kokku leppida. COBITi seitse teabekriteeriumi on järgmised:

- toimivus,
- tõhusus,
- konfidentsiaalsus,
- terviklus,

- käideldavus,
- vastavus,
- teabe usaldatavus.

2.1.8 Kui IS audiitor on varem osalenud rakendussüsteemi väljatöötamises, hankimises, evituses või hoolduses ning talle määratakse auditiülesanne, võib ta sõltumatus osutuda küsitavaks. Sellistel juhtudel peaks IS audiitor toetuma asjakohastele suunistele.

3 AUDITITÖÖ SOORITAMINE

3.1 Tehinguvoo dokumenteerimine

3.1.1 Kogutav teave peaks hõlmama nii süsteemi automatiseeritud kui ka käsitoimingute aspekte. Keskenduda tuleks auditi eesmärgi jaoks olulisele andmesisestusele (elektroonilisele ja käsitsi sooritatavale), -töötlusele, -talletusele ja -väljastusele. Tehinguvoo dokumenteerimine sõltub talitlusprotsessidest ja tehnoloogia kasutamisest ning IS audiitor võib teatud juhtudel leida, et dokumenteerimine ei ole praktiline. Sellisel juhul peaks IS audiitor koostama andmevoo üldjoonelise skeemi või kirjelduse ja/või kasutama süsteemi dokumentatsiooni, kui see on tema käsutuses. Tuleb mõelda ka rakenduse ja muude süsteemide vaheliste liideste dokumenteerimisele.

3.1.2 IS audiitor võib dokumentatsiooni kinnitada näiteks läbikõnnitestiga või muu protseduuriga.

3.2 Rakendussüsteemi turvameetmete väljaselgitamine ja kontroll

3.2.1 IS audiitor võib välja selgitada spetsiifilised meetmed rakenduse riskide leevendamiseks ning hankida piisavad auditi asitõendid kinnituse saamiseks selle kohta, et meetmed toimivad kavatsetud viisil. Seda võimaldavad teha näiteks järgmised protseduurid:

- küsitlus ja vaatlus;
- dokumentatsiooni läbivaatus;
- rakendussüsteemi turvameetmete testimine programmeeritud meetmete kontrollimisel; võib kaaluda CAAT-vahendite kasutamist.

3.2.2 Kontrollimise iseloom, ajastus ja ulatus peaksid põhinema vaadeldava ala riskitasemel ja auditi eesmärkidel. Tugevate üldiste IT meetmete puudumisel võib IS audiitor hinnata selle nõrkuse mõju rakenduse arvutipõhiste meetmete usaldatavusele.

3.2.3 Kui IS audiitor leiab rakenduse arvutipõhistes meetmetes olulisi nõrkusi, peaks ta võimaluse korral otsima kinnitust (kui seda nõuab auditi eesmärk) käsitöötluse turvameetmetest.

G14 Rakendussüsteemide läbivaatus (jätkub)

3.2.4 Arvutipõhiste meetmete toimivus sõltub üldiste IT meetmete tugevusest. Kui üldisi IT meetmeid läbi ei vaadata, on seetõttu võib-olla tunduvalt vähem võimalik toetuda rakenduse meetmetele ja IS audiitor peaks kaaluma alternatiivseid protseduure.

4 ARUANDLUS

4.1 Nõrkused

4.1.1 Rakenduse läbivaatusel avastatud nõrkused, mis on tingitud turvameetmete puudumisest või mittevastavusest, tuleks teha teatavaks talitlusprotsessi omanikule ja rakenduse toe eest vastutavale IS juhtkonnale. Kui rakendussüsteemi läbivaatusel avastatud nõrkused loetakse olulisteks või kaalukateks, tuleks vastava taseme juhtkonnale soovitada rakendada viivitamatult parandusmeetmeid.

4.1.2 Kuna rakenduse arvutipõhiste meetmete toimivus sõltub üldistest IT meetmetest, tuleks teatada ka üldiste meetmete nõrkustest. Kui üldisi meetmeid läbi ei vaadatud, tuleks see asjaolu märkida aruandesse.

4.1.3 IS audiitor peaks aruandes esitama asjakohased soovitused meetmete tugevdamiseks.

5 JÕUSTUMISKUUPÄEV

5.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. novembril 2001 või pärast seda.

G15 Plaanimine

1 TAUST

1.1 Seos ISACA standarditega

1.1.1 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.2 Suunise vajadus

1.2.1 Selle suunise eesmärk on määratleda IS auditeerimisstandardile S5 vastava plaanimisprotsessi komponendid.

1.2.2 See suunis tagab ka auditiprotsessi plaanimise nii, et saavutataks COBITi eesmärgid.

2 PLAANIMINE

2.1 Talitlusnõuded

2.1.1 See suunis hõlmab ühtainsat auditeerimisprojekti, mitte auditiosakonna või -grupi täielikku plaani.

2.1.2 IS audiitor peaks koostama auditi plaani, mis võtab arvesse auditiala ja selle tehnoloogilise infrastruktuuri seisukohalt asjassepuutuva auditeeritava eesmärgid. Vajaduse korral peaks IS audiitor arvestama ka läbivaadatavat ala ja selle seost organisatsiooniga (strateegilist, rahalist ja/või talitluslikku) ning hankima teavet strateegilise plaani kohta, sealhulgas IS strateegilise plaani kohta.

2.1.3 Suutmaks kavandada plaani, mis sobib auditeeritava praeguse või vajadusel ka tulevase tehnoloogia puhul, peaks IS audiitor saama ettekujutuse auditeeritava infoarhitektuurist ja tehnoloogilisest suunitlusest.

2.1.4 Lähtetingimused peaksid olema üks osa auditi plaanist.

2.1.5 Vajalikus ulatuses tuleks läbivaatuse all oleva ala ja organisatsiooni IS-keskkonna kohta kaalutleda riskid ja määrata tuvastatud riskidele prioriteedid. Vt IS auditeerimise suunis G13 "Riski kaalutlemise kasutamine auditi plaanimisel".

2.2 Organisatsiooni tundmine

2.2.1 Enne auditeerimisprojekti alustamist tuleks IS audiitori töö plaanida auditi eesmärkide saavutamiseks sobival viisil. Plaanimisprotsessi ühe osana peaksid IS audiitorid õppima tundma organisatsiooni ja ta protsesse. See annab IS audiitoritele ettekujutuse organisatsiooni tegevusest ja ta IS-nõuetest, peale selle aga aitab IS audiitoril teha kindlaks läbivaadatavate IS-ressursside tähtsust organisatsiooni eesmärkide seisukohalt. IS audiitorid peaksid ka välja selgitama auditi tööd käsitlusala ning sooritama läbivaadatava funktsiooni sisejuhtimise eelhindamise.

G15 Plaanimine (jätkub)

2.2.2 Kui palju peab IS audiitor tundma organisatsiooni ja ta protsesse, sõltub organisatsiooni iseloomust ja sooritamisele kuuluva audititöö detailsusastmest. Ebaharilike või keeruliste operatsioonide käsitlemisel peab IS audiitoril võib-olla olema eriteadmisi. Kui auditi eesmärk hõlmab infosüsteemide funktsioonide laia skaalat, on harilikult vaja tunda organisatsiooni ja ta protsesse põhjalikumalt kui piiratud arvu funktsioonide järgi seatud eesmärgi puhul. Näiteks läbivaatus, mille eesmärk on hinnata organisatsiooni palgalehesüsteemi ohjet, nõuab harilikult põhjalikumat organisatsiooni tundmist kui läbivaatus, mille eesmärk on teatava programmiteegisüsteemi ohjemeetmete testimine.

2.2.3 IS audiitor peaks saama ettekujutuse sedalaadi sündmustest, tehingutest ja tavadest, mis võivad oluliselt mõjutada auditeerimisprojekti objektiks olevat konkreetset organisatsiooni, funktsiooni, protsessi või andmestikku. Organisatsiooni tundmine peaks hõlmama organisatsiooni ähvardavaid tegevusalaseid, rahalisi ja olemuslikke riske ning organisatsiooni turu olukorda. Audiitoril tuleks ka teada, millises ulatuses sõltub organisatsioon oma eesmärkide saavutamisel väljasttellimisest. Seda teavet peaks IS audiitor kasutama võimalike probleemide tuvastamiseks, töö eesmärkide ja käsitlusala sõnastamiseks, töö sooritamiseks ning juhtkonna selliste toimingute arvestamiseks, mille suhtes IS audiitor peaks olema valvas.

2.3 Kaalukus

2.3.1 Plaanimisprotsessis peaks IS audiitor tavaliselt määrama sellised kaalukuse plaanimise tasemed, et audititöö oleks piisav auditi eesmärkide saavutamiseks ning kasutaks auditi ressursse tõhusalt. Näiteks mingi olemasoleva süsteemi läbivaatusel hindab IS audiitor sooritatava töö auditikava plaanimisel süsteemi mitmesuguste komponentide kaalukust. Kaalukuse määramisel peaks IS audiitor arvestama nii kvalitatiivseid kui ka kvantitatiivseid aspekte. Lisateabe saamiseks kaalukuse kohta vt IS auditeerimise suunis G6 "Olulisuse kontseptsioonid infosüsteemide auditeerimisel".

2.4 Riski kaalutlemine

2.4.1 Mõistliku kinnituse saamiseks sellele, et audititöö käigus kaetakse kaalukad aspektid adekvaatselt, tuleks sooritada riski kaalutlemine. See kaalutlemine peaks välja selgitama need kohad, kus on suhteliselt suur kaalukate probleemide olemasolu risk.

2.5 Sisejuhtimise hindamine

2.5.1 Auditeerimisprojektid peaksid sisaldama sisemeetmete kaalumist otseselt auditeerimisprojekti eesmärkide ühe osana või alusena toetumiseks teabele, mida kogutakse auditeerimisprojekti ühe osana. Kui eesmärk on sisemeetmete hindamine, peaks IS audiitor mõtlema sellel, millises ulatuses on vaja sellised meetmed läbi vaadata. Kui eesmärk on hinnata meetmete toimivust mingil ajavahemikul, peaks auditi plaan sisaldama auditi eesmärkide saavutamiseks sobivaid protseduure ning need protseduurid peaksid sisaldama meetmete vastavuse kontrollimist. Kui eesmärgiks ei ole hinnata meetmete toimivust mingil ajavahemikul, vaid tuvastada juhtimisprotseduurid mingil hetkel, võib meetmete vastavuse kontrolli välja jätta.

G15 Plaanimine (jätkub)

2.5.2 Kui IS audiitor hindab sisemeetmeid eesmärgiga toetuda juhtimisprotseduuridele, mis toetavad teavet, mida kogutakse auditi osana, peaks ta harilikult sooritama nende meetmete eelhindamise ning koostama selle hindamise põhjal auditi plaani. Läbivaatuse ajal kaalub IS audiitor selle hindamise sobivust otsustamisel, mil määral võib testimise ajal toetuda nendele meetmetele. Näiteks kui IS audiitor kasutab andmefailide testimiseks programme, peaks ta hindama meetmeid, mida rakendatakse programmiteekidele, mis sisaldavad auditi eesmärkidel kasutatavaid programme, et otsustada, mil määral on need programmid kaitstud volitamata muudatuste eest.

3 DOKUMENTATSIOON

3.1 Plaanimisdokumentatsioon

3.1.1 IS audiitori töödokumentide hulka peaksid kuuluma auditi plaan ja kava.

3.1.2 Auditi plaani võib dokumenteerida paberil või mingil muul sobival ja leitaval kujul.

3.2 Plaani kinnitamine

3.2.1 Auditi plaani, auditi kava ja kõiki järgnevaid muudatusi peaks sobivas ulatuses kinnitama auditi juhtkond.

3.3 Auditi kava

3.3.1 Enne töö alustamist peaks IS audiitor tavaliselt koostama läbivaatuse esialgse kava. Auditi kava tuleks dokumenteerida nii, et IS audiitor saaks protokollida audititöö lõpetamise ja piiritleda töö, mis jääb veel teha. Töö edenemisel peaks IS audiitor auditi käigus kogutud teabe põhjal hindama kava adekvaatsust. Kui IS audiitor otsustab, et plaanilised protseduurid ei ole piisavad, peaks ta vastavalt sellele muutma kava.

3.3.2 Kui auditiressursside vajadus seda nõuab, peaks IS audiitor võtma auditi plaani vajalike personaliressursside halduse.

3.3.3 Auditi plaan tuleks koostada nii, et ta peale IS auditeerimise standardite nõuetele vastaks ka kõigile asjakohastele välistele nõuetele.

3.3.4 Lisaks vajalike tööde loetelule peaks IS audiitor kasulikus ulatuses koostama ka töö sooritamiseks vajaliku personali- ja muude ressursside loetelu, töö ajakava ja eelarve.

3.3.5 Töö käigus peaks IS audiitor kava adekvaatsuse hindamise ja oma esialgsete leidude põhjal kaaluma muudatuste tegemist auditi kavas.

4 JÕUSTUMISKUUPÄEV

4.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. märtsil 2002 või pärast seda.

G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele

1 TAUST

1.1 Seos ISACA standarditega

1.1.1 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.2 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.2 Määratlused

1.2.1 ISP – Interneti-teenuse tarnija. Kolmas pool, kes annab organisatsioonile mingil kujul Interneti ja Internetiga seotud teenused.

1.2.2 ASP/MSP – rakenduste või hallatud teenuste tarnija. Kolmas pool, kes Interneti või privaatvõrgu kaudu tarnib ja haldab paljudele kasutajatele rakendusi ja arvutiteenuseid, sealhulgas turvateenuseid.

1.2.3 BSP – talitlusteenuste tarnija. ASP, kes annab ka väljasttellitavaid talitlusprotsesse, näiteks maksete töötlust, tellimuste töötlust ja rakenduste väljatöötamist.

1.2.4 Selles suunises on ISP-de, ASP/MSP-de ja BSP-de koondnimetusena kasutatud terminit "kolmandad pooled". Selle suunisega hõlmatud kolmandate poolte hulka kuulub iga organisatsioon (näiteks ühiskasutuslike teenuste organisatsioonid), mis on auditeeritavast organisatsioonist lahus, olgu ta juriidiliselt lahus või mitte.

1.3 Suunise rakendamine

1.3.1 Selle suunise rakendamisel peaks IS audiitor võtma arvesse ta juhised koos muude asjassepuutuvate ISACA suunistega.

1.4 Suunise vajadus

1.4.1 See suunis määrab, kuidas IS audiitor kolmanda poole mõju hindamisel organisatsiooni infosüsteemide juhtimismeetmetele ja nendega seotud juhtimiseesmärkidele peaks järgima ISACA standardeid ja COBITit.

1.4.2 See suunis ei ole mõeldud andma juhiseid selle kohta, kuidas IS audiitori aruanne kolmandast poolest tarnija meetmete kohta peaks vastama muude standardimisorganite nõuetele.

G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele (jätkub)

2 KOLMANDATEST POOLTEST TEENUSETARNIJATE ROLL

2.1 Kolmandatest pooltest tarnijate teenused

2.1.1 Organisatsioonid kasutavad mitmesugustel eesmärkidel Internetti ja üleorganisatsioonilisi sisevõrke. Nende eesmärkide hulka kuulub töötajate, tarnijate ja klientide juurdepääs olemasolevatele ja /või uutele inimressursi-, rahandus-, turustus- ja hankimisrakendustele. Paljudel juhtudel antakse see juurdepääs ühe või mitme kolmandast poolest tarnija kaudu.

2.1.2 Kolmandad pooled võivad anda näiteks järgmisi teenuseid:

- sisemiste võrkude ühendamine Internetiga;
- organisatsiooni partnerite ühendamine virtuaalsete privaatvõrkude või partnerivõrkude kaudu;
- klientide ühendamine traadita tehnoloogia abil;
- veebisaidi väljatöötamine;
- veebisaidi hooldus, haldus ja seire;
- veebisaidi turbe teenused;
- füüsilise asukoha andmine riistvara jaoks (riistvara majutus);
- süsteemi ja rakenduste juurdepääsu seire;
- varunduse ja taaste teenused;
- rakenduste väljatöötamine, hooldus ja majutamine (näiteks ettevõtte ressursside plaanimise süsteemid, e-kaubanduse süsteemid);
- äriteenused, näiteks rahahalduse, krediitkaardi-, tellimuste töötluse ja konsultatsioonipunkti teenused.

3 MÕJU MEETMETELE

3.1 Kolmandatest pooltest tarnijate mõju meetmetele

3.1.1 Kui organisatsioon kasutab kolmandaid pooli, võivad need muutuda organisatsiooni meetmete ja vastavate juhtimiseesmärkide otsustavaks komponendiks.

3.1.2 IS audiitor peaks hindama rolli, mida kolmas pool täidab IT-keskkonna ning sellega seotud meetmete ja juhtimiseesmärkide alal.

3.1.3 Kui organisatsioon kasutab kolmandatest pooltest tarnijaid piiratud otstarbeks, näiteks riistvaramajutuse teenuste saamiseks, võib ta oma juhtimiseesmärkide saavutamisel toetuda neile kolmandatele pooltele ainult piiratud otstarbel.

G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele (jätkub)

3.1.4 Kui aga organisatsioon kasutab tarnijaid muudeks otstarveteks, näiteks raamatupidamise või e-kaubanduse süsteemide majutuseks, kasutab ta oma juhtimiseesmärkide saavutamiseks täielikult või koos enda meetmetega kolmandast poolest tarnija meetmeid.

3.1.5 Kolmanda poole meetmete toimivus võib tugevdada organisatsiooni võimet saavutada oma juhtimiseesmärke, ja vastupidi, toimetud kolmanda poole meetmed võivad nõrgendada organisatsiooni võimet saavutada oma juhtimiseesmärke. Niisugustel nõrkustel võivad olla mitmesugused allikad, sealhulgas järgmised:

- juhtimiskeskkonna lüngad, mis tekivad teenuste tellimisest kolmandatelt pooltelt;
- meetmete halb lahendus, mistõttu meetmed ei toimi;
- meetmete toimivuse eest vastutajate puudulikud teadmised või kogemused;
- ülemäärane sõltuvus kolmanda poole meetmetest (kui organisatsioonis ei ole mingeid korvavaid meetmeid).

4 IS AUDIITORI PROTSEDUURID

4.1 Tundmaõppimine

4.1.1 Plaanimisprotsessis peaks IS audiitor endale selgeks tegema ja dokumenteerima seose kolmanda poole antavate teenuste ja organisatsiooni juhtimiskeskkonna vahel. IS audiitor peaks mõtlema selliste asjade läbivaatusele nagu kolmanda poole ja organisatsiooni vaheline leping, teenusetasemelepe, poliitikad ja protseduurid.

4.1.2 IS audiitor peaks dokumenteerima need kolmanda poole protsessid ja meetmed, mis otseselt mõjutavad organisatsiooni protsesse ja juhtimiseesmärke.

4.1.3 IS audiitor peaks välja selgitama iga meetme, selle asukoha ühendatud juhtimiskeskkonnas (sisemine või väline), meetme tüübi, meetme funktsiooni (vältiv, avastav või parandav) ning organisatsiooni, kes täidab seda funktsiooni (sisemine või väline).

4.1.4 IS audiitor peaks kaalutlema riski, mis tuleneb kolmanda poole teenustest organisatsioonile, ta meetmetest ja juhtimiseesmärkidest, ning määrama kolmanda poole meetmete tähtsusest organisatsiooni võimele saavutada oma juhtimiseesmärke.

4.2 Ettekujutusele kinnituse saamine

4.2.1 IS audiitor peaks saama kinnituse oma ettekujutusele juhtimiskeskkonnast.

4.2.2 IS audiitor võib oma ettekujutusele juhtimiskeskkonnast saada kinnituse mitmesuguste meetoditega, näiteks küsitlustega, vaatlustega ja tehingute läbikõndidega.

G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele (jätkub)

4.3 Kolmandast poolest tarnija meetmete rolli hindamine

4.3.1 Kui kolmandal poolel on oluline roll või mõju organisatsiooni juhtimiseesmärkidele, peaks IS audiitor hindama neid meetmeid otsustamiseks, kas nad töötavad, nagu on kirjeldatud, kas nad toimivad ja kas nad aitavad organisatsioonil saavutada juhtimiseesmärke.

5 KOLMANDATEST POOLTEST TARNIJATEGA SEOTUD RISKID

5.1 Kolmandatest pooltest tarnijate mõju organisatsioonile

5.1.1 Kolmandatest pooltest tarnijad võivad paljudel tasemetel mõjutada organisatsiooni (ja ta partnereid), ta protsesse, meetmeid ja juhtimiseesmärke. Selliste mõjude allikad võivad olla näiteks järgmised:

- kolmandast poolest tarnija majanduslik eluvõime;
- kolmandast poolest tarnija juurdepääs teabele, mis edastatakse tema sidesüsteemide ja rakenduste kaudu;
- süsteemide ja rakenduste käideldavus;
- töötluse terviklus;
- rakenduste väljatöötamise ja muutusehalduse protsessid;
- süsteemide ja infovarade kaitse varunduse ja taastega, ootamatuste käsitluse plaanimisega ja liiasusega.

5.1.2 Meetmete puudumise ja/või meetmete lahenduse, töötamise või toimimise nõrkuste tulemusteks võivad olla näiteks

- teabe konfidentsiaalsuse ja privaatsuse kadu;
- süsteemide kättesaamatus kasutamiseks, kui neid vajatakse;
- volitamatu juurdepääs süsteemidele, rakendustele ja andmetele ja nende volitamata muutmine;
- süsteemide, rakenduste või andmete muudatused, mis tulenevad süsteemide või turvalisuse riketest, andmete kaotsiminekust, andmetervikluse kadumisest, andmete kaitse kadumisest või süsteemide käideldamatusest;
- süsteemi ressursside ja/või infovarade kaotsiminek;
- kõigest ülalloetletust tingitud suuremad kulud organisatsioonile.

5.2 Meetmetes tuvastatud nõrkuste hindamine

5.2.1 IS audiitorid peaksid hindama IT-keskkonna meetmete rakendatuse, lahenduse või töötamise nõrkuste tõenäosust (või juhtimisriski). IS audiitor peaks välja selgitama, kus leidub meetmete nõrkusi.

G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele (jätkub)

5.2.2 Seejärel peaks IS audiitor hindama, kas juhtimisrisk on oluline ja kuidas ta mõjutab juhtimiskeskkonda.

5.2.3 Kui nõrkused on tuvastatud, peaks IS audiitor tegema kindlaks, kas tuvastatud nõrkuste toime vastu on olemas korvamismeetmed (need võivad olla organisatsioonis, kolmandast poolest tarnijal või mõlemal). Kui korvamismeetmed on olemas, peaks IS audiitor välja selgitama, kas nad leevendavad tuvastatud meetmenõrkuste toimet.

6 LEPINGUD KOLMANDATEST POOLTEST TARNIJATEGA

6.1 Rollid ja kohustused

6.1.1 Organisatsiooni ja kolmandast poolest tarnija vahelised suhted peaksid olema dokumenteeritud täidetava lepingu kujul. See leping on organisatsiooni ja teenusetarnija suhetes elutähtis element. Niisugused lepingud sisaldavad palju sätteid, mis suunavad mõlema poole toiminguid ja kohustusi.

6.1.2 IS audiitor peaks organisatsiooni ja kolmanda poole vahelise lepingu läbi vaatama.

6.1.3 Selle suunise kontekstis peaks IS audiitor selle lepingu läbi vaatama (võib-olla organisatsiooni juristi abiga), et teha kindlaks kolmanda poole roll ja kohustused organisatsiooni abistamisel ta juhtimiseesmärkide saavutamiseks. Juhised selle kohta, kuidas lepinguid läbi vaadata, jäävad väljapoole käesoleva suunise käsitlusala, kuid järgnev loetelu esitab näiteid küsimustest, millele IS audiitor peaks mõtlema lepingu läbivaatamisel.

- Teenusetase, mille peab tagama kolmas pool (organisatsioonile ja/või selle partneritele).
- Kolmanda poole kehtestatud tasu mõistlikkus.
- Kohustused andmete ja rakenduste privaatsuse ja konfidentsiaalsuse alal.
- Kohustused süsteemide, side, operatsioonisüsteemide, utiliitide, andmete ja rakendustarkvara pääsu reguleerimise ja halduse alal.
- Varade ja nendega seotud andmete seire ning reageerimise (organisatsioonis ja kolmandal poolel) ja aruandluse protseduurid (rutiinsed ja intsidendiprotseduurid).
- Infovarade (sealhulgas andmete ja domeeninimede) omanike spetsifitseerimine.
- Organisatsiooni tellimusel kolmandas pooles väljatöötatavate programmide, sealhulgas muudatuste dokumentatsiooni, lähtekoodi ja hoiustuslepingute omanike spetsifitseerimine.
- Sätted süsteemide ja andmete kaitse kohta, sealhulgas varunduse ja taaste, ootamatuste käsitluse plaanimise ning liiasuse kohta.

G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele (jätkub)

- Auditeerimisõiguse säte (mis hõlmab näiteks võimalust kohtuda kolmandapoolse tarnija siseauditi talituse töötajatega ning läbi vaadata nende sooritatud auditite töödokumente ja aruandeid).
- Lepingu ja sellega seotud dokumentide (näiteks teenusetasemelepete ja protseduuride) muudatuste läbirääkimise, läbivaatuse ja kinnitamise protsess.

6.1.4 Et teha kindlaks, mil määral vastutab kolmas pool nende meetmete eest, mida ta rakendab organisatsiooni huvides, peaks IS audiitor vähemalt läbi vaatama lepingu. See protsess peaks hindama tuvastatud meetmete ning nende vastavuse seire ja aruandluse piisavust, lahendust ja rakendamise toimivust.

6.2 Organisatsioonipoolne haldus

6.2.1 Ka siis, kui on mängud kolmandatest pooltest tarnijad, on asjakohaste juhtimiseesmärkide saavutamine üha juhtkonna kohus. Selle kohustuse ühe osana peaks juhtkonnal olema protsess, millega hallata kolmandapoolse tarnija sooritust ja suhteid selle tarnijaga. IS audiitor peaks selle protsessi komponendid välja selgitama ja läbi vaatama. IS audiitor peaks muuhulgas läbi vaatama protsessi, mida juhtkond kasutab kolmandapoolse tarnijaga kaasnevate riskide tuvastamiseks, kolmanda poole antavad teenused ja selle, kuidas juhtkond haldab suhteid kolmanda poolega.

6.2.2 IS audiitori sooritatav haldusprotsessi läbivaatus peaks andma kinnituse sellele, kas juhtkond vaatab läbi kolmandapoolseid tarnijaid selliste sooritusstandardite või -kriteeriumide alusel, mis on sätestatud lepingus ja kõigis regulatiivsete organite spetsifitseeritud standardites. Haldusprotsess peaks sisaldama muuhulgas alljärgneva läbivaatust:

- kolmandast poolest tarnija rahanduslikud tulemused;
- lepingutingimuste täitmine;
- muudatused juhtimiskeskkonnas, mida on nõudnud kolmas pool ja ta audiitorid ja/või regulatiivorganid;
- teiste, sealhulgas kolmanda poole audiitorite, konsultantide jt sooritatud meetmeläbivaatuste tulemused;
- pidev kindlustus adekvaatsel tasemel.

7 KOLMANDAST POOLEST TARNIJA MEETMETE LÄBIVAATUS

7.1 Lepinguküsimused

7.1.1 Kolmandast poolest tarnija meetmete läbivaatamisel peaks IS audiitor võtma arvesse organisatsiooni ja kolmandast poolest tarnija vahelise lepingulise suhte ning kolmandast poolest tarnija enda hindamised ja aruandluse oma meetmete kohta.

G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele (jätkub)

7.1.2 Lepinguküsimused võivad takistada IS audiitorit läbi vaatamast meetmeid kolmanda poole juures. Sellisel juhul peaks IS audiitor hindama sellist kitsendust enda võimalustele hinnata infosüsteemide juhtimiskeskkonda.

7.2 Sõltumatud aruanded

7.2.1 Kolmandatest pooltest tarnijad võivad esitada oma meetmete kohta sõltumatutest allikatest pärit aruandeid. Neil aruandeil võib olla teenusebüroo auditiaruande või muu meetmepõhise aruande kuju. IS audiitorid võivad neid aruandeid kasutada alusena, mille põhjal toetuda infosüsteemide juhtimiskeskkonna meetmetele.

7.2.2 Kui IS audiitor otsustab kasutada sõltumatut aruannet alusena, mille põhjal toetuda infosüsteemide meetmetele kolmandast poolest tarnija juures, peaks ta need aruanded läbi vaatama alljärgneva kontrollimiseks.

- Sõltumatu pool on kvalifitseeritud. See võib hõlmata järgmist: sõltumatul poolel on asjakohane kutsealane tunnistus või litsents, tal on asjassepuutuvad kogemused ning ta on heas kirjas vastavates kutsealastes ja regulatiivsetes (kui on kohaldatav) organites.
- Sõltumatul poolel pole kolmandast poolest tarnijaga mingeid selliseid suhteid, mis võiksid kahjustada nende sõltumatust ja objektiivsust.
- Aruandega kaetud periood.
- Aruanne on piisav (st aruanne katab asjassepuutuvad süsteemid ja meetmed ning sisaldab nende alade kontrollimist, mida IS audiitor oleks kontrollinud, kui ta oleks ise sooritanud selle töö).
- Meetmete kontrollimine on piisav võimaldamaks IS audiitoril toetuda selle sõltumatu poole tööle (st meetmete kontrollimine ning sooritatud protseduuride iseloom, ajastus ja ulatus on piisavad).
- Aruanne teeb vahet teenuseandja kohustuste ja kasutava organisatsiooni kohustuste vahel.
- Kasutav organisatsioon on täitnud oma kohustused õigete meetmete alal.

7.3 Kolmanda poole meetmete kontrollimine

7.3.1 Kui IS audiitor otsustab otseselt läbi vaadata meetmed kolmandast poolest tarnija juures ja neid kontrollida, peaks ta

- selle ürituse plaanimiseks, eesmärkide seadmiseks ja läbivaatuse käsitlusala määramiseks tegema koostööd mõlema organisatsiooni juhtkonnaga ja (kui see on võimalik ja vajalik) nende siseauditi talitusega;
- hoolitsema juurdepääsu saamise eest kolmanda poole süsteemidele ja varadele, samuti konfidentsiaalsuse eest;

G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele (jätkub)

- koostama auditi kava, eelarve ja ürituse plaani;
- valideerima juhtimiseesmärke.

7.3.2 Kui IS audiitor on lõpetanud kontrollimistöö, tuleks teha kokkuvõte kontrollitud meetmete toimivuse kohta. IS audiitor peaks läbi vaatama meetmete toimivuse kummaski organisatsioonis ja ka meetmete vastastikuse toime organisatsiooni ja kolmanda poole vahel.

7.3.3 Enamikul juhtudel organisatsiooni ja kolmandast poolest tarnija meetmed osaliselt kattuvad. IS audiitor peaks hindama meetmete toimivust koos vaadelduna, võrreldes seda eraldi rakendamisega.

7.3.4 Võib ka esineda olukordi, kus meetmed mingi konkreetse eesmärgi taotlemiseks ühes neist organisatsioonidest puuduvad või ei toimi. Sellisel juhul peaks IS audiitor hindama selle nõrkuse mõju kogu juhtimiskeskkonnale ja selle protseduuride ulatusele.

7.3.5 Võib esineda ka olukordi, kus ühe organisatsiooni meetmete tugevust võivad osaliselt või täielikult vähendada meetmete nõrkused teises organisatsioonis. Sellises olukorras on IS audiitori kohus hinnata kogu juhtimiskeskkonda.

7.4 Kolmandast poolest tarnija siseaudiitorid

7.4.1 IS audiitor peaks mõtlema ka sellele, kas kolmandast poolest tarnijal on siseauditi osakond. Siseaudiitorite olemasolu kolmandast poolest tarnijal võib tugevdada kolmandast poolest tarnija juhtimiskeskkonda.

7.4.2 Kui siseauditi osakond on olemas, peaks IS audiitor tegema kindlaks siseaudiitorite tegevuse ulatuse organisatsiooni mõjutavate süsteemide ja meetmete osas.

7.4.3 Kui võimalik, peaks IS audiitor läbi vaatama asjassepuutuvad kolmandast poolest tarnija siseauditi aruanded.

7.4.4 Juhtudel, kui neid aruandeid ei ole võimalik läbi vaadata, peaks IS audiitor arutama nende läbivaatuste käsitlusala, selgitama välja, millised süsteemid ja meetmed kaeti nende läbivaatustega ning millised olulised küsimused ja nõrkused tuvastati.

7.4.5 Kui kolmandast poolest tarnija ei soovi anda juurdepääsu oma siseauditi personali aruannetele, peaks IS audiitor hindama selle kitsenduse mõju oma protseduuride ulatusele.

7.4.6 IS audiitor peaks kaaluma ka kolmandast poolest tarnija siseauditi personali oskuste ja kogemuste hindamist. Selleks võib vestelda nende inimestega või kasutada lisaprotseduure, näiteks nende tööplaanide, töödokumentide ja aruannete läbivaatust.

G16 Kolmandate poolte mõju organisatsiooni IT-meetmetele (jätkub)

8 KOLMANDATE POOLTE ALLETTEVÕTJAD

8.1 Mõju meetmetele

8.1.1 IS audiitor peaks kindlaks tegema, kas kolmas pool kasutab süsteemide ja teenuste tarnimiseks allettevõtjaid.

8.1.2 Juhul, kui allettevõtjaid kasutatakse, peaks IS audiitor läbi vaatama nende allettevõtjate tähtsuse ja tegema kindlaks, milline võib olla nende mõju kolmanda poole esmastele meetmetele, mis on seotud vaadeldava organisatsiooniga.

8.2 Mõju ülesandele

8.2.1 Kui allettevõtja oluliselt ei mõjuta organisatsioonisse puutuvaid meetmeid, peaks IS audiitor selle asjaolu dokumenteerima oma töödokumentides.

8.2.2 Kui allettevõtja oluliselt mõjutab organisatsioonisse puutuvaid meetmeid, peaks IS audiitor hindama protsesse, millega kolmas pool haldab ja seirab oma suhteid allettevõtjaga. Nende meetmete hindamisel, mida kolmas pool rakendab oma allettevõtjaile, peaks IS audiitor arvestama selle suunise jaotisi 6 ja 7.

9 ARUANDLUS

9.1 Nõrkused

9.1.1 IS audiitori aruanne peaks näitama, et läbivaatuse objektiks olnud meetmed hõlmavad meetmeid auditeeritavas organisatsioonis ja meetmeid kolmanda poole organisatsioonis. Peale selle peaks IS audiitor mõtlema kummaski organisatsioonis olevate meetmete, nende nõrkuste ja korvavate meetmete väljaselgitamisele.

9.1.2 Järelduste ja soovituste esitamise ulatus peaks olema dokumenteeritud lähtetingimustes. Mõned organisatsioonid ei taha või ei suuda soovitusi ellu viia. Sellistel juhtudel peaks IS audiitor soovitama korvavaid meetmeid, mida organisatsioon võiks rakendada kolmanda poole organisatsiooni meetmete nõrkuste kõrvaldamiseks.

10 JÕUSTUMISKUUPÄEV

10.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. märtsil 2002 või pärast seda.

G17 Auditivälise rolli mõju IS audiitori sõltumatusele

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S2 "Sõltumatus" määrab: "Kõigis auditiga seotud küsimustes peaks IS audiitor olema auditeeritavast sõltumatu nii oma hoiakult kui ka esinemiselt."

1.1.2 Standard S2 "Sõltumatus" määrab: "IS auditi talitus peaks auditiülesande objektiivseks sooritamiseks olema piisavalt sõltumatu läbivaadatavast tegevusvaldkonnast."

1.2 Suunise vajadus

1.2.1 Paljudes organisatsioonides ootavad juhtkond, IT-personal ja siseauditi talitus, et IS audiitoritel võib olla muid, mitte auditialaseid rolle, näiteks järgmiste hulgast:

- IS strateegiate määratlemine tehnoloogia, rakenduste ja ressursside alal;
- tehnoloogiate hindamine, valimine ja rakendamine;
- kolmandatelt pooltelt pärit IS-rakenduste ja -lahenduste hindamine, valimine, kohandamine ja evitamine;
- tellimustööna valmistatavate IS-rakenduste ja -lahenduste kavandamine, väljatöötamine ja teostamine;
- mitmesuguste IS funktsioonidega seotud parimate tavade, poliitikate ja protseduuride loomine;
- turbe ja juhtimise kavandamine, väljatöötamine ja rakendamine.

1.2.2 Üldiselt tähendab auditiväline roll täiskohaga või osa-ajaga osalemist IS-üritustes ja IS projektirühmades töö sooritajana või nõuandja või konsultandina. Näiteid:

- IS auditi personali ajutine täiskohaga määramine või laenamine IS projektirühma;
- IS auditi personali osa-ajaga määramine mitmesuguste projektistruktuuride, näiteks projekti juhtrühma, projekti töörühma, hindamisrühma, läbirääkimis- ja lepingurühma, teostusrühma, kvaliteedi tagamise rühma või rikkeotsingu rühma liikmeks;
- ebaregulaarne tegutsemine sõltumatu nõuandjana või läbivaatajana.

1.2.3 Sellised auditivälised rollid on tähtis osa IS audiitori panusest teiste organisatsiooni liikmete koolitusest. Nad võimaldavad IS audiitoritel kasutada oma asjatundmist ja organisatsiooni tundmist ainulaadse ja hinnalise panuse andmiseks organisatsiooni IS-investeeringute toimivusse ja tõhususse. Nad võimaldavad ka tõsta IS auditi talituse profiili ning annavad IS auditi personalile hinnalisi praktilisi kogemusi.

1.2.4 Kui IS audiitor on osalenud mingis IS-ürituses auditivälises rollis, samal ajal või hiljem aga auditeeriti seda üritust või sellega seotud IS-funktsiooni, võivad sellest

auditist tulenenud soovitused ja järeldused tunduda nende saajatele ebaobjektiivsed. Selles olukorras võib tunduda, et auditiväline osalus on kahjustanud IS audiitori sõltumatust ja objektiivsust.

1.2.5 Käesoleva suunise eesmärk on anda raamstruktuur, mis võimaldaks IS audiitoril

- otsustada, millal võib nõutav sõltumatus olla puudulik või näida olevat puudulik;
- kaaluda võimalikke alternatiivseid lähenemisi auditiprotsessile, kui nõutav sõltumatus on puudulik või näib olevat puudulik;
- määrata avalikustamisnõudeid.

2 AUDITITALITUSE PÕHIKIRI

2.1 IS audiitorite auditivälise osaluse tingimused

2.1.1 IS auditi põhikiri peaks kehtestama mandaadi IS audiitori osaluseks auditivälistes rollides ning selliste rollide üldise iseloomu, ajastuse ja ulatuse. See väldiks vajadust anda konkreetseid mandaate juhtumhaaval.

2.1.2 IS audiitor peaks andma mõistliku kinnituse sellele, et konkreetsete auditiväliste rollide pädevustingimused on kooskõlas audititalituse põhikirjaga. Võimalike lahknevuste puhul peaksid need lahknevused olema pädevustingimustes selgelt sõnastatud.

3 SÕLTUMATUS

3.1 Sõltumatuse relevantsus auditivälistes rollides

3.1.1 Auditeerimise standard S2 nõuab, et IS audiitor oleks sõltumatu "kõigis auditiga seotud küsimustes". Kui seda ei keela muud välised standardid, ei ole IS audiitorile mingeid nõudeid olla või näida sõltumatu, kui ta osalus IS-ürituses vastab iseloomult ühele neist auditivälistest rollidest, mis on visandatud jaotises 1.2.1 ülal.

3.1.2 Auditivälise rolliga seotud ülalnimetatud ülesannete täitmisel ei pea IS audiitor küll olema sõltumatu, kuid endiselt kehtib kutsealane objektiivsuse nõue. IS audiitor peaks täitma auditivälise rolliga seotud ülesandeid objektiivselt, ratsionaalselt ja nihketa.

3.1.3 IS-ürituses auditivälise rolli täitmisel ei nõuta küll IS audiitorilt sõltumatust, kuid ta peaks mõtlema sellele, kas niisugune roll ei kahjusta ta sõltumatust siis, kui IS audiitorile tehakse ülesandeks auditeerida seda IS-üritust või sellega seotud funktsiooni. Kui võib oodata sellist vastuolu (näiteks kui hiljem nõutakse sõltumatut auditit, kuid on ainult üks IS audiitor, kellel on vajalikud oskused nii auditivälise rolli ja ka järgneva auditi tarbeks), peaks IS audiitor enne auditivälisesse rolli asumist arutama seda küsimust auditikomisjoniga või sellele vastava juhtimisüksusega.

G17 Auditivälise rolli mõju IS audiitori sõltumatusele (jätkub)

3.1.4 IS-ürituses täidetava auditivälise rolli ning IS-ürituse või sellega seotud funktsiooni sõltumatu auditi vahelise kompromissi peaks otsustama auditikomisjon või sellele vastav juhtimisüksus. Seda otsust mõjutavad tõenäoliselt järgmised aspektid:

- võimalikud alternatiivsed ressursid ükskõik kumba rolli jaoks;
- vastuolus olevate tegevustega lisatava suhtelise väärtuse tajumine;
- potentsiaal IS-rühma koolitamiseks, nii et sellest oleks kasu tulevastel üritustel;
- IS audiitori karjääri arendamise võimalused ja ametijärglase plaanimine;
- auditivälise rolliga kaasneva riski suurus;
- mõju IS auditi talituse nähtavusele, profiilile, kuvandile jne;
- otsuse mõju võimalike väliste audiitorite või reguleerijate nõuetele;
- IS auditi talituse põhikirja sätted.

3.2 Auditiväliste rollide mõju järgnevatele auditite

3.2.1 Kui mingit IS-üritust või -funktsiooni auditeeritakse põhikirja ja/või juhtkonna nõuete alusel, peaks IS audiitor olema ja näima sõltumatu IS-rühmast ja selle juhtkonnast.

3.2.2 IS audiitori auditiväline osalemine mingis IS-ürituses võib potentsiaalselt kahjustada tema sõltumatust selle IS-ürituse ja temaga seotud funktsiooni auditeerimise seisukohalt. IS audiitor peaks deklareerima, kas tema arvates ta auditiväline roll kahjustab või ei kahjusta tema sõltumatust auditi sooritamisel. Auditikomisjonilt või sellele vastavalt juhtimisüksuselt tuleks taotleda selle arvamuse kirjalikku kinnitust.

3.2.3 Oluliste tegurite hulka, mis võivad aidata otsustada, kas IS audiitori auditiväline roll võib kahjustada tema sõltumatust mingi auditi seisukohalt või mitte, kuuluvad näiteks järgmised aspektid.

- IS audiitori auditivälise rolli iseloom, ajastus ja ulatus IS-ürituses, mille audit või millega seotud funktsiooni audit on kõne all. Mida suurem on auditivälise rolli otsustusõigus, seda tugevamalt kahjustab see sõltumatust.
- Sõltumatust õõnestavatena tunduda võivate faktide olemasolu. Niisuguste hulka võivad kuuluda sellised aspektid nagu auditivälise rolliga seotud materiaalne hüve või karistus.
- IS audiitori võime ja kohustumus jääda auditi läbiviimisel ning nõrkustest või vigadest teatamisel nihutamatuks ja erapooletuks, vaatamata oma auditivälisele rollile.

G17 Auditivälise rolli mõju IS audiitori sõltumatusele (jätkub)

- IS audiitori vabadus otsustada auditi käsitlusala ja läbiviimist, vaatamata enda osalusele auditivälises rollis.
- IS audiitori poolne auditivälise rolli, selles osalemise määra ja sellega seotud kaalukate faktide avalikustamine.

4 PLAANIMINE

4.1 Mõju sõltumatusele

4.1.1 Auditiväliste rollide plaanimisel tuleks hinnata auditivälise rolli võimalikku mõju sõltumatusele sama IS-ürituse või sellega seotud funktsiooni tõenäolise tulevase või samaaegse auditi seisukohalt.

4.1.2 IS audiitori varasemast või jätkuvast osalusest auditivälises rollis mingis IS-ürituses tulenevat võimalikku mõju ta sõltumatusele tuleks igasuguste selletaoliste IS-ürituste või nendega seotud funktsioonide auditite plaanimisel hinnata.

4.1.3 Nagu on mainitud jaotistes 3.1.3 ja 3.2.2, tuleks olukordades, millele on viidatud jaotistes 4.1.1 ja 4.1.2, informeerida auditikomisjoni või talle vastavat juhtimisüksust võimalikust sõltumatuse kahjustusest. Auditikomisjoni või talle vastava juhtimisüksuse informeerimisel võimalikust kahjustusest peaks IS audiitor soovitama meetmeid, mida võiks rakendada mõistliku kinnituse andmiseks sõltumatuse ja objektiivsuse kohta, sealhulgas järgmisi.

- Lisaks IS audiitorile, kellel on olnud või on auditiväline roll, määrata IS auditi talitusest selliseid täiendavaid juhte ja/või töötajaid, kellel pole olnud auditeerimisele kuuluval alal mingit auditivälist rolli.
- Lisaks IS audiitorile, kellel on olnud või on auditiväline roll, määrata juhte ja töötajaid väljastpoolt IS auditi talitust, näiteks laenata personali teisest talitusest või osakonnast, välisest organisatsioonist jne.
- Partnerläbivaatuse sooritamiseks ning plaanimise, välitöö ja aruandluse käigus sõltumatu vahekohtunikuna tegutsemiseks määrata sõltumatu ressurss IS auditi talitusest või muudest ülalviidatud allikatest.

5 AUDITITÖÖ SOORITAMINE

5.1 Auditi läbiviimise seire

5.1.1 Sellise auditi puhul, kus on olemas sõltumatuse kahjustamise võimalus auditivälise osaluse tõttu, peaks IS auditi juhtkond auditi läbiviimist hoolikalt seirama. IS auditi juhtkond peaks kriitiliselt hindama sõltumatuse kõiki auditivälisest osalusest tingitud kahjustuse kaalukaid ilminguid ning algatama vajalikud parandustoimingud. Sellistel juhtudel tuleks informeerida auditikomisjoni või talle vastavat juhtimisüksust.

G17 Auditivälise rolli mõju IS audiitori sõltumatusele (jätkub)

6 ARUANDLUS

6.1 Avalikustamisnõuded

6.1.1 Kui IS auditi juhtkonna ja/või töötajate sõltumatus mingi IS-ürituse või sellega seotud funktsiooni auditi seisukohalt võib auditivälise rolli tõttu selles IS-ürituses olla või tunduda olevat kahjustatud, peaks IS audiitor auditi aruandes avalikustama piisavalt teavet auditivälise rolli kohta ning meetmete kohta, mida on rakendatud mõistliku kinnituse saamiseks objektiivsusele. See võimaldab auditi aruande kasutajail saada ettekujutust võimaliku kahjustuse tõenäolisest ulatusest ja selle kahjustuse mõjude leevendamiseks rakendatud meetmetest. Teave, mille avalikustamisele peaks mõtlema IS audiitor, hõlmab järgmisi aspekte:

- IS-ürituses auditivälises rollis osalenud IS auditi juhtkonna ja töötajate nimed ja ametiastmed;
- IS-ürituses auditivälise osalemise iseloom, ajastus ja ulatus;
- põhjused nende osalemiseks IS-ürituses auditivälises rollis ja selle IS-ürituse või sellega seotud funktsiooni auditis;
- sammud, mida on astutud kinnituse andmiseks sellele, et auditi töö ja aruandluse käigus ei ole objektiivsust kaalukalt kahjustatud;
- fakt, et sõltumatuse võimalik kahjustus on teatavaks tehtud auditikomisjonile või sellele vastavale juhtimisüksusele ning enne auditivälise rolli täitmist on neilt saadud nõusolek.

7 JÕUSTUMISKUUPÄEV

7.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. juulil 2002 või pärast seda.

G18 IT haldus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite asjakohase analüüsi ja tõlgendamisega."

1.2 Suunise vajadus

1.2.1 COBITi® annotatsioon määrab: "Organisatsioonid peavad täitma kvaliteedi-, rahandus- ja turvanõudeid oma teabele nii, nagu kõigi varade puhul. Juhtkond peab ka optimeerima nende käsutuses olevate ressursside, sealhulgas andmete, rakendussüsteemide, tehnoloogia, rajatiste ja inimeste kasutamist. Nende kohustuste täitmiseks ja oma eesmärkide saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimissüsteemi."

1.2.2 Tehnika kasutamine majanduslike ja sotsiaalsete ettevõtmiste kõigis aspektides on tekitanud elutähtsa sõltuvuse infotehnoloogiast majanduslike tehingute, teabe ja teadmiste kõigi aspektide algatamiseks, jäädvustamiseks, teisalduseks ja halduseks, luues ettevõtte halduses IT halduse jaoks elutähtsa koha.

1.2.3 Laia kõlapinnaga probleemid (näiteks süsteemide tõrked viirusrünnete tõttu, usalduse või süsteemide käideldavuse kadu veebisaitide häkkimise tõttu), mida on tulnud kogeda mitmesugustel avaliku ja erasektori organisatsioonidel, on tõmmanud tähelepanu ettevõtte haldamise küsimustesse. Formaalsed vahendid, millega juhtkond täidab oma kohustusi organisatsiooni käitus- ja rahandustegevuste sisejuhtimise toimiva süsteemi rajamiseks, võivad olla avaliku jälgimise objektiks ning sageli moodustavad nad nii sise- kui ka välisaudiitoritele auditi käsitlusala ühe osa.

1.2.4 Käesoleva suunise eesmärk on anda teavet selle kohta, kuidas peaks IS audiitor lähenema IT halduse auditile, ning ta hõlmab sellise IS audiitori asjakohast organisatsioonilist positsiooni, asjaolusid, mida arvestada auditi plaanimisel, ning asitõendeid, mida läbi vaadata auditi sooritamisel. See suunis annab juhiseid ka aruandluse adresseerimise ja sisu kohta ning auditijärgse töö kohta, mida tuleb arvestada.

2 AUDITITALITUSE PÕHIKIRI

2.1 Mandaat

2.1.1 IT haldus kui üks ettevõtte halduse valdkondi kujutab endast selliste aspektide kogumit, mida tuleb käsitleda siis, kui vaadeldakse, kuidas ettevõttes infotehnoloogiat rakendatakse. IT on praegu ettevõtetes olemuslik ja kõikehõlmav, mitte ettevõtte muu osa suhtes marginaalne eraldi talitus. Sellel, kuidas ettevõttes infotehnoloogiat rakendatakse, on tohutu mõju sellel, kas ettevõte saavutab oma missiooni, nägemuse

või strateegilised sihid. Seetõttu on ettevõttel vaja hinnata oma IT haldust, kuna see muutub kogu ettevõtte halduse üha tähtsamaks osaks. Aruandlus IT halduse kohta hõlmab auditeerimist organisatsiooni kõrgeimal tasemel ning võib ületada ettevõtte harude, tegevusliinide ja osakondade piire. IS audiitor peaks veenduma, et lähtetingimustes on määratud

- töö käsitlusala, sealhulgas auditiga kaetavate funktsionaalsete alade ja aspektide selge määratlus;
- alluvusliin, mida tuleb kasutada, kui IT halduse aspekte identifitseeritakse organisatsiooni kõrgeima tasemeni;
- IS audiitori õigus saada juurdepääsu teabele.

3 SÕLTUMATUS

3.1 Organisatsiooniline staatus

3.1.1 IS audiitor peaks mõtlema sellele, kas tema organisatsiooniline staatus sobib plaanitud auditi iseloomuga. Kui ta arvab, et mitte, peaks juhtkonna vastav tase kaaluma sõltumatu kolmanda poole palkamist selle auditi haldamiseks või sooritamiseks.

4 PLAANIMINE

4.1 Faktiotsing

4.1.1 IS audiitor peaks hankima teavet IT halduse struktuuri kohta, sealhulgas nende tasemete kohta, kelle kohus on

- hallata ettevõtet;
- seada ettevõttele strateegilised suunad;
- hinnata tegevjuhataja (-juhatuse) sooritust ettevõtte strateegiate elluviimisel;
- hinnata kõrgema juhtkonna ja strateegiate rakendamise (sealhulgas sellega seotud teadmuse, teabe ja tehnoloogia) eest vastutavate alluvate sooritust;
- otsustada, kas ettevõte on välja arendanud talle seatud strateegiliste sihtide saavutamiseks vajalikud oskused ja infrastruktuuri;
- hinnata ettevõtte võimet jätkata oma senist tegevust.

4.1.2 IS audiitor peaks välja selgitama ja endale üldjoontes selgeks tegema protsessid, mis võimaldavad IT halduse struktuuril täita jaotises 4.1.1 loetletud ülesandeid, samuti suhtluskanalid, mille abil seatakse sihte ja eesmärke madalamatele tasemetele (ülalt alla) ja saadakse teavet nende vastavuse seireks (alt üles).

G18 IT haldus (jätkub)

4.1.3 IS audiitor peaks hankima teavet organisatsiooni infosüsteemide strateegia kohta (olgu see dokumenteeritud või mitte), sealhulgas järgnevat:

- pika ja lühikese tähtajaga plaanid organisatsiooni missiooni ja sihtide saavutamiseks;
- pika ja lühikese tähtajaga strateegia ja plaanid IT-le ja süsteemidele nende plaanide toetamiseks;
- metoodika IT strateegia väljatöötamiseks, plaanide koostamiseks ja edenemise seireks nende plaanidega võrreldes;
- IT strateegia ja plaanide muutmise reguleerimise metoodika;
- IT missiooni määrang ning kokkulepitud sihid ja eesmärgid IT-tegevustele;

seniste IT-tegevuste ja süsteemide hindamised.

4.2 IS auditi eesmärgid

4.2.1 IT halduse auditi eesmärke võivad mõjutada sihtgrupi vajadused ja kavatsetava levituse tase. Auditi üldiste eesmärkide seadmisel peaks IS audiitor mõtlema järgmistele valikutele:

- aruandlus haldussüsteemi ja/või ta toimivuse kohta;
- rahandusteabe süsteemide katmine või väljajätmine;
- mitterahandusliku teabe süsteemide katmine või väljajätmine.

4.2.2 IT halduse IS-auditi detailsed eesmärgid sõltuvad harilikult sisejuhtimise raamstruktuurist, mida kasutab tippjuhtkond. Kui sellist väljakujunenud raamstruktuuri ei ole, tuleks detailsete eesmärkide seadmise miinimumalusena kasutada COBITi raamstruktuuri.

4.3 Auditi käsitlusala

4.3.1 IS audit peaks auditi käsitlusalasse võtma asjassepuutuvad IT-tegevuse plaanimise ja organiseerimise protsessid ning selle tegevuse seire protsessid.

4.3.2 Auditi käsitlusalasse peaksid kuuluma kõigi COBITi raamstruktuuris määratletud varade kasutamise ja kaitse juhtimissüsteemid. Need varad on

- andmed,
- rakendussüsteemid,
- tehnoloogia,
- rajatised,
- inimesed.

G18 IT haldus (jätkub)

4.4 Töötajad

4.4.1 IS audiitor peaks saama mõistliku kinnituse sellele, et niisuguse läbivaatuse sooritamiseks kasutatavail töötajail on asjakohane juhtiv positsioon ja pädevus.

5 AUDITITÖÖ SOORITAMINE

5.1 Tippjuhtkonna tegevuste läbivaatus

5.1.1 IT haldust kui ettevõtte halduse üht osa peaksid suunama ettevõtte tegevuse sihid ja eesmärgid. Tegevuse strateegilise plaanimise protsessi olemasolu hindamiseks peaks IS audiitor arvestama seda, kas

- on olemas tegevuse visiooni ja missiooni selge määratlus;
- on kasutusel tegevuse strateegilise plaanimise metoodika;
- selles protsessis osalejate tase on asjakohane;
- seda plaanimist ajakohastatakse regulaarselt.

5.1.2 IT strateegilise plaanimise protsessi läbivaatamisel peaks IS audiitor arvestama, kas

- on olemas IT visiooni ja missiooni selge määratlus;
- on kasutusel strateegilise IT plaanimise metoodika;
- see metoodika seob tegevuse sihid ja eesmärgid IT sihtide ja eesmärkidega;
- seda plaanimisprotsessi ajakohastatakse regulaarselt (vähemalt kord aastas);
- see plaan piiritleb peamised IT-üritused ja vajalikud ressursid;
- selles protsessis osalejate tase on asjakohane.

5.1.3 IT taktikalise plaanimise läbivaatamisel peaks IS audiitor vaatlema kasutuselolevaid projektihalduse tavasid, võttes arvesse

- kasutatavate projektihalduse meetodite ulatuse;
- rakendatavad projektihalduse meetmed;
- kasutatavad projektihalduse instrumendid;
- IT ja põhitegevuse personali integratsiooni projektide eri järkudes;
- organisatsioonis olulisi muudatusi tegevate suurte projektide puhul kasutatavad muudatuste halduse metoodikad.

G18 IT haldus (jätkub)

5.1.4 Väljastusprotsessi läbivaatamisel peaks IS audiitor võtma arvesse

- kasutuselolevad käitusmeetmed (COBITi eesmärgid, mis on seotud rakenduse arendusega;
- arendus- või muutmisprotsessi;
- projektihalduse protsessi (nagu seda on käsitletud jaotises 5.1.3).

5.1.5 Keskendumisel rakenduste arendamise metoodikale ja tavadele ning meetmetele, mida rakendatakse arendusprotsessile võib IS audiitor võtta läbivaatusele alljärgneva.

- Rakenduse väljatöötamise metoodika (kaaludes selle kvaliteeti: näiteks, kas see on tugevalt struktureeritud ja katab süsteemiarenduse elutsükli kõiki järke ning arvestab keskkonna iseärasusi, näiteks väljasttellimist või hajussüsteeme).
- Projekti mahu ja projekti edenemise hindamiseks kasutatav arendusmõõdustik.
- Meetodid, millega uuritakse testimisprobleeme, õpitakse neist ning täiustatakse metoodikat ja meetmeid tulevaste projektide tarbeks.

5.1.6 Praeguse süsteemistiku halduseks kasutatavate protsesside läbivaatamisel peaks IS audiitor arvestama organisatsiooni strateegiliste ja tugialade kaetust praeguste süsteemidega. IS audiitor võib võtta läbivaatusele alljärgneva.

- Tegevuse strateegilise plaanimise protsessis määratletud strateegiliste alade üldine kaetus kehtestatud poliitikatega.
- Protsess, mida tippjuhtkond järgib poliitikale vastavuse detailiseerimiseks, teatavakstegemiseks, nõudmiseks ja seireks.
- Dokumenteeritud poliitikad järgneva kohta, vastavalt vajadusele: turvalisus, inimressursid, andmete omandus, lõppkasutaja andmetöötlus, intellektuaalne omand, andmete säilitus, süsteemide hankimine ja evitamine, väljasttellimine, sõltumatu kinnitus, jätkusuutlikkuse plaanimine, kindlustus, privaatsus.
- Läbivaadatavates protsessides osalejate (näiteks andmete omanikud, IT juhtkond, täitevjuhtkond) rollide ja kohustuste määratlus. Otsustada, kas need sobivad läbivaadatavate protsesside toetamiseks.
- Kas läbivaadatavates protsessides osalejatel on oma rollide täitmiseks vajalikud oskused, kogemused ja ressursid?
- Kas siseaudit on vajalikul tasemel kaasatud (kui organisatsioonil on sisemisi auditiressursse)?
- Hinnata, kas organisatsiooni IT-spetsialistide või IT-talituse positsioon on sobiv ja võimaldab organisatsioonil oma tegevuseesmärkide saavutamiseks IT kõige paremini ära kasutada.

G18 IT haldus (jätkub)

- Hinnata, kas IT-spetsialistide ja IT-kohustustega mittespetsialistide organisatsioon ja juhtimine on adekvaatne käsitlema vigadest, tegematajätmistest, korratustest ja ebaseaduslikest toimingutest tulenevaid riske organisatsioonile.

5.1.7 IS audiitor peaks mõtlema sellele, kas ülalnimetatud läbivaatustega kogutud auditi asitõenditega on vajalikud alad kaetud. Küsimused, mida tuleks käsitleda, on määratud COBITi IT halduse suunises. See suunis hõlmab keskseid sihiindikaatoreid, kriitilisi edutegureid ja keskseid sooritusenäitajaid, mis suunavad IT haldust ta sihtide poole. Näiteid teabest, mida tuleks arvestada:

- IT missiooni määrangu ning IT-tegevuste kokkulepitud sihtide ja eesmärkide olemasolu;
- organisatsiooni IT-ressursside kasutamisega seotud riskide hinnang ja nende riskide haldamise metoodika;
- IT strateegia plaanid strateegia elluviimiseks ja edenemise seireks võrdluses nende plaanidega;
- IT eelarved ja hälvete seire;
- IT kasutamise ja kaitse üldised poliitikad ning nende poliitikate järgimise seire;
- asjassepuutuvate IT sooritusenäitajate võrdlus, näiteks mõõtlusväärtustega analoogilistest organisatsioonidest või talitustest, sobivatest rahvusvahelistest standarditest, küpsusmudelitest või tunnustatud parimatest tavadest;
- soorituse regulaarne seire kokkulepitud sooritusnäitajate järgi;
- asitõendid haldustalituse perioodiliste IT läbivaatuste kohta, kusjuures tegutsemist nõudvad probleemid on välja selgitatud, ülesandeks tehtud, lahendatud ja jälitatud;
- asitõendid toimivate ja mõttekate sidemete kohta nende protsesside vahel, mida kirjeldavad jaotised 5.1.1 - 5.1.5 ülal.

5.1.8 IS audiitor peaks kindlaks tegema, kas tippjuhtkond on algatanud IT suhtes asjakohased haldustegevused ning kas neid tegevusi seiratakse asjakohaselt.

6 ARUANDLUS

6.1 Adressaadid

6.1.1 IS audiitor peaks aruanded IT halduse kohta adresseerima auditikomisjonile ja tippjuhtkonnale.

6.1.2 Kui IT halduses tuvastatakse puudusi, tuleks neist viivitamatult teatada asjakohasele auditi põhikirjas määratletud isikule või grupile.

G18 IT haldus (jätkub)

6.2 Sisu

6.2.1 Auditi aruanne IT halduse kohta peaks vastama teistele ISACA standarditele ning aruandes peaksid vastavalt lähtetingimustele olema

- lausung selle kohta, et tippjuhtkond vastutab organisatsiooni sisejuhtimise süsteemi eest;
- lausung selle kohta, et sisejuhtimine saab anda mõõdukat, mitte absoluutset kaitset vääresituste või kahjude eest;
- toimiva IT halduse süsteemi saamiseks tippjuhtkonna kehtestatud kesksete protseduuride ja nendega seotud abidokumentatsiooni kirjeldus;
- teave kõigi lahknevuste kohta organisatsiooni poliitikatest või kohaldatavatest õigusnormidest või tegevusala ettevõttehalduse tavade koodeksitest;
- teave kõigi suuremate ohjamata riskide kohta;
- teave kõigi mittetoimivate või ebatõhusate juhtimisstruktuuride, meetmete või protseduuride kohta, koos IS audiitori täiustussoovitustega;
- IS audiitori üldine järeldus IT halduse kohta, vastavalt lähtetingimustes olevale määratlusele.

7 JÄRELTOIMINGUD

7.1 Õigeaegsus

7.1.1 Ettevõtte halduse süsteemi iga nõrkuse toimed on harilikult laiaulatuslikud ja tekitavad suure riski. Seetõttu peaks IS audiitor vajaduse korral aegsasti sooritama piisava järeltöö, kontrollimaks, kas juhtkond on viivitamatult rakendanud meetmeid nõrkuste käsitlemiseks.

8 JÕUSTUMISKUUPÄEV

8.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. juulil 2002 või pärast seda.

G19 Korratused ja ebaseaduslikud toimingud

1 TAUST

1.1 Seos ISACA standarditega

1.1.1 Standard S3 "Kutse-eetika ja standardid" määrab: "IS audiitor peaks auditiülesannete täitmisel järgima ISACA kutse-eetika koodeksit."

1.1.2 Standard S3 "Kutse-eetika ja standardid" määrab: "IS audiitor peaks ilmutama vajalikku kutsealast hoolikust, sealhulgas järgima kohaldatavaid kutsealaseid auditeerimise standardeid."

1.2 Suunise vajadus

Selle suunise eesmärk on anda IS audiitorile juhiseid korratuste ja ebaseaduslike toimingute määratlemise kohta ning töö sooritamisel arvestatava kohta.

2 MÄÄRATLUSED

2.1 Korratused ja ebaseaduslikud toimingud

2.1.1 Korratuste ja ebaseaduslike toimingute hulka võivad kuuluda

- pettus, st igasugune toiming, mis sisaldab petmist ebaseadusliku kasu saamiseks;
- muud toimingud, mis sisaldavad lahknemist õigusnormidest, sealhulgas ka IT-süsteemide suutmatus järgida kehtivaid õigusnorme;
- toimingud, mis sisaldavad lahknemist organisatsiooni kokkulepetest ja lepingutest kolmandate pooltega, näiteks pankade, tarnijate ja müüjatega;
- andmike või dokumentide (elektroonilisel või paberkujul) manipuleerimine, võltsimine või muutmine;
- tehingute toimete vähendamine või väljajätt kirjetest või dokumentidest (elektroonilisel või paberkujul);
- fiktiivsete tehingute kirjendamine organisatsiooni rahalistes või muudes andmikes (elektroonilisel või paberkujul);
- IS-varade või muude varade volitamatu kasutamine või väärkasutus;
- muud toimingud, mis on sihilikud, kuid mitte pettuslikud rikkumised, sealhulgas kaubamärgi-, autori- ja patendiõiguste rikkumised;
- sellised vead organisatsiooni rahalistes või muudes andmikes, mida põhjustab volitamatu juurdepääs organisatsiooni IT-süsteemidele või nende süsteemide volitamata kasutamine.

2.1.2 Korratuste hulka ei kuulu, kui need pole ülal määratletud teisiti, kõik organisatsiooni lahknevused halduspoliitikatest ega organisatsiooni väär käitumine oma tegevuse sooritamisel.

G19 Korratused ja ebaseaduslikud toimingud (jätkub)

2.2 Sõltuvus õiguslikust otsusest

2.2.1 Küsimus selle kohta, kas on leidnud aset korratus, ebaseaduslik toiming või viga, ning milline on selle kaalukus või mõju organisatsioonile, jääb väljapoole IS audiitori käsitlusala ja kohustusi.

2.2.2 Otsus selle kohta kas mingi(d) toiming(ud) on ebaseaduslik(ud), põhineb üldiselt asjaga kursis oleva kvalifitseeritud juristi nõuandel, võib-olla aga on võimalik alles pärast lõpliku kohtulahendini jõudmist.

2.2.3 Lihtsuse mõttes räägib see juhend "korratustest ja ebaseaduslikest toimingutest", ehkki praktikas tuleb IS audiitoril harilikult tegeleda mitte tõestatud, vaid kahtlustatava pettuse või muude ebaseaduslike toimingutega.

3 JUHTKONNA JA IS AUDIITORI KOHUSTUSED

3.1 Juhtkond

3.1.1 Juhtkonna kohus on vältida ja avastada korratusi ja ebaseaduslikke toiminguid.

3.1.2 Mõistliku kinnituse saamiseks sellele, et korratused ja ebaseaduslikud toimingud välditakse või aegsasti avastatakse, kasutab juhtkond harilikult järgmisi vahendeid:

- sisemeetmeid, sealhulgas tehingute läbivaatuse, kinnitamise ja juhtkondliku läbivaatuse protseduure;
- poliitikaid ja protseduure, mis suunavad töötajate käitumist;
- vastavuse valideerimise ja seire protseduure.

3.1.3 IS audiitor peaks aga mõistma, et juhtimismehhanismid ei välista korratuste või ebaseaduslike toimingute võimalust.

3.2 IS audiitor

3.2.1 IS audiitori kutsealane kohus ei ole vältida ega avastada korratusi või ebaseaduslikke toiminguid.

3.2.2 Seetõttu, välja arvatud niisuguse teabe olemasolul, mis näitab IS audiitorile, et on leidnud aset korratus või ebaseaduslik toiming, ei ole IS audiitor kohustatud sooritama protseduure, mis on spetsiaalselt mõeldud korratuste või ebaseaduslike toimingute avastamiseks.

3.2.3 IS audiitori kohustus uurida korratusi ja teatada neist tekib ainult olukorras, kus tuvastatakse asitõendid korratuse või ebaseadusliku toimingu kohta.

3.2.4 IS audiitor peaks informeerima juhtkonda ja auditikomisjoni (või sellele vastavat) ka siis, kui ta tuvastab olukordi, kus võib tekkida suurem korratuste või ebaseaduslike toimingute (ehkki neid ei ole avastatud) risk.

G19 Korratused ja ebaseaduslikud toimingud (jätkub)

3.2.5 Ülesande lähtetingimustes võidakse aga esitada IS audiitorile erinõue sooritada protseduure, mis on mõeldud korratuste või ebaseaduslike toimingute avastamiseks.

4 ÜLESANDE PLAANIMINE JA SOORITAMINE

4.1 Ülesande plaanimine

4.1.1 IS audiitor ei ole küll otseselt kohustatud avastama ega vältima ebaseaduslikke toiminguid või korratusi, kuid ta peaks kavandama ebaseaduslike toimingute ja korratuste avastamise protseduure ebaseaduslike toimingute ja korratuste esinemise riski suuruse hinnangu põhjal.

4.1.2 Seetõttu peaks IS audiitor ülesande plaanimisel saama ettekujutuse sellistest aspektidest nagu

- sisejuhtimise keskkond;
- töötajate käitumist suunavad poliitikad ja protseduurid;
- vastavuse valideerimise ja seire protseduurid;
- õiguskeskkond, milles tegutseb organisatsioon;
- mehhanism, mida organisatsioon kasutab teda mõjutavate õigusaktide hankimiseks, seireks ja järgimiseks.

4.1.3 Seejärel peaks IS audiitor kaalutlema riski, mille tekitab see, et võivad leida aset aruande objekti seisukohalt kaalukad korratused või ebaseaduslikud toimingud.

4.1.4 Riskide kaalutlemisel tuleks võtta arvesse ainult need tegurid, mis on organisatsiooni ja ülesande objekti seisukohalt asjakohased, sealhulgas näiteks

- rahalise arvestuse andmikke mõjutavate korratuste või ebaseaduslike toimingutega seotud riskitegurid;
- rahalise arvestuse andmikke mitte mõjutavate, kuid organisatsiooni mõjutavate korratuste või ebaseaduslike toimingutega seotud riskitegurid;
- organisatsiooni meetmete piisavusse puutuvate korratuste või ebaseaduslike toimingutega seotud riskitegurid.

4.1.5 Riskide kaalutlemisel peaks IS audiitor võtma arvesse ka muud tegurid, mis võivad mõjutada neid riske, sealhulgas näiteks

- töötajate rahulolematuse mõju;
- võimalikud koondamised, väljasttellimised, ettevõtte osaline müük või restruktureerimine;
- volitamata kasutamisele altide varade olemasolu;
- organisatsiooni halvad rahalised ja/või tegevusalased tulemused;
- juhtkonna hoiak eetika suhtes;

G19 Korratused ja ebaseaduslikud toimingud (jätkub)

- korratused ja ebaseaduslikud toimingud, mis on levinud teatud tegevusalal või on aset leidnud sarnastes organisatsioonides.

4.1.6 Plaanimisprotsessi ja riski kaalutlemise ühe osana peaks IS audiitor küsitlema juhtkonda järgmistel teemadel.

- Juhtkonna ettekujutus organisatsioonis korratuste ja ebaseaduslike toimingutega tekitatava riski suurusest.
- Kas juhtkonnale on teada korratusi või ebaseaduslikke toiminguid, mis leidsid aset või võisid leida aset organisatsiooni vastu või organisatsiooni sees?
- Kuidas seiratakse ja hallatakse korratuste või ebaseaduslike toimingute riski?

4.2 Ülesande protseduurid

4.2.1 IS audiitor peaks ülesande jaoks kavandama protseduurid, mis võtavad arvesse korratuste ebaseaduslike toimingute riski tuvastatud suuruse.

4.2.2 Riski kaalutlemise ja muude plaanimise ajal sooritatud protseduuride tulemusi tuleks kasutada ülesande käigus sooritatavate protseduuride iseloomu, ulatuse ja ajastuse määramiseks.

4.2.3 IS audiitor peaks küsitlema ka IT ja kasutajate juhtkonda (vastavalt vajadusele) õigusnormide järgimise asjus.

4.3 Ülesande protseduuride tulemuste hindamine

4.3.1 IS audiitor peaks läbi vaatama ülesande protseduuride tulemused ja tegema kindlaks, kas võis ilmneda märke korratustest või ebaseaduslikest toimingutest.

4.3.2 Kui see hindamine on sooritatud, tuleks jaotises 4.1 loetletud riskitegurid tegelike sooritatud protseduuride põhjal uuesti läbi vaadata mõistliku kinnituse saamiseks sellele, et kõiki tuvastatud riske on käsitletud.

4.3.3 Hindamine peaks sisaldama ka protseduuride tulemuste kaalutlemist eesmärgiga teha kindlaks, kas on mingeid dokumenteerimata riskitegureid.

5 KORRATUSTE VÕI EBASEADUSLIKE TOIMINGUTE AVASTAMISEL

5.1 Reageerimine võimalikele ebaseaduslikele toimingutele

5.1.1 Kui IS audiitorile saab teatavaks võimalikku ebaseaduslikku toimingut puudutav teave, peaks ta mõtlema sellele, et

- saada ettekujutus toimingu iseloomust;
- saada ettekujutus selle toimumise asjaoludest;

G19 Korratused ja ebaseaduslikud toimingud (jätkub)

- hankida korratuse või ebaseadusliku toimingu mõju hindamiseks piisavat muud teavet;
- sooritada lisaprotseduure, millega teha kindlaks korratuse või ebaseadusliku toimingu mõju ja see, kas on veel teisi selliseid toiminguid.

5.1.2 Korratuse või ebaseadusliku toimingu esinemise ja mõju väljaselgitamiseks peaks IS audiitor tegema organisatsioonis koostööd teistega (näiteks organisatsiooni turvapersonaliga), sealhulgas juhtkonnaga (kui võimalik, siis sobival osalejatest kõrgemal tasemel).

5.2 Sooritatavad protseduurid

5.2.1 Ülesande täitmise käigus võivad IS audiitorile ilmneda märgid korratuste või ebaseaduslike toimingute olemasolust. Kui on leitud ebaseadusliku toimingu märke, peaks IS audiitor mõtlema, kuidas võib toiming mõjutada ülesande objekti, aruannet ja organisatsiooni.

5.2.2 Kui on tuvastatud võimalik korratus või ebaseaduslik toiming, peaks IS audiitor organisatsioonis konsulteerima juristiga või muude asjakohaste inimestega. Kas mingi toiming on tõepoolest korratus või ebaseaduslik akt, saab otsustada ainult jurist.

5.2.3 Kui asjaolud ei näita selgelt vastupidist, peaks IS audiitor eeldama, et korratus või ebaseaduslik toiming ei ole üksikjuhtum.

5.2.4 IS audiitor peaks ka läbi vaatama asjassepuutuvad osad organisatsiooni sisemeetmetest ja välja selgitama, miks need ei suutnud vältida või avastada korratuse või ebaseadusliku toimingu juhtumit.

5.2.5 IS audiitor peaks uuesti vaatlema organisatsiooni sisemeetmete piisavuse, kasutamise ja toimivuse algset hindamist.

5.2.6 Kui IS audiitor on tuvastanud olukordi, kus ilmneb korratus või ebaseaduslik toiming (potentsiaalne või tegelik), peaks ta muutma sooritatavaid protseduure, et saada tuvastatud probleemile ülesande sooritamise käigus kinnitust või lahendada see probleem.

5.2.7 Niisuguste muudatuste või lisaprotseduuride ulatus sõltub sellest, millised on IS audiitori arvates

- võimaliku korratuse või ebaseadusliku toimingu tüüp;
- tajutav selle esinemise risk;
- võimalik mõju organisatsioonile, sealhulgas rahaline ja mõju organisatsiooni mainele;
- analoogiliste korratuste või ebaseaduslike toimingute kordumise tõenäosus;
- tõenäosus, et juhtkond võib olla korratusest või ebaseaduslikust toimingust teadlik või olla sellesse segatud;
- võimalikud meetmed, mida rakendab juhtimisüksus ja/või juhtkond;
- tõenäosus, et lahknevus õigusnormidest ei ole sihilik;

- tõenäosus, et lahknevuse tõttu võidakse kohaldada kaalukat trahvi või muud sanktsiooni, näiteks võidakse tühistada oluline litsents;
- korratusest tuleneda võiv mõju ühiskonna huvidele.

5.3 Juhtkond

5.3.1 Kui korratusse on segatud juhtkonna liige, peaks IS audiitor uuesti läbi mõtlema juhtkonnapoolsete esituste usaldatavuse.

5.3.2 Tüüpiliselt peaks IS audiitor tegema koostööd sobiva juhtkonnatasemega, mis on kõrgemal korratuse või ebaseadusliku toiminguga seotud juhtkonnast.

6 ARUANDLUS

6.1 Teatamine korratustest ja ebaseaduslikest toimingutest

6.1.1 Korratuste ja ebaseaduslike toimingute kaalukus ja võimalik mõju aruande objektile varieeruvad tugevalt.

6.1.2 Korratuse või ebaseadusliku toimingu mõjude hindamine tuleks sooritada koostöös juristiga ja vajaduse korral võib-olla koos organisatsiooni juhtimisüksusega (näiteks direktsiooni või auditikomisjoniga) või juhtkonnaga.

6.1.3 Hindamine peaks arvestama, kuidas mõjutab korratus või ebaseaduslik toiming kehtivaid kokkuleppeid, lepinguid ja õigusakte.

6.1.4 Korratuse või ebaseadusliku toimingu võimalik mõju objektile ja aruandele varieerub sõltuvalt ebaseadusliku toimingu tüübist ja organisatsiooni tegevuse iseloomust.

6.1.5 Kui ei nõuta teisiti, on IS audiitori kohus teatada ainult toimingut ümbritsevatest sündmustest ja asjaoludest.

6.1.6 Juhtkonna kohus on, tavaliselt juristiga konsulteerides, teha kindlaks ja teatada, kas toiming on tõepoolest korratus või ebaseaduslik toiming.

6.1.7 Mõnedes jurisdiktsioonides võib IS audiitoril olla lisakohustusi, mis ulatuvad kaugemale jaotises 6.1.5 ülal spetsifitseeritud nõuetest. Sellisel juhul peab IS audiitor andma mõistliku kinnituse sellele, et ta järgib ka neid lisanõudeid.

6.2 Aruanded juhtkonnale

6.2.1 IS audiitor peaks esitama aruandes nende sündmuste ja asjaolude kirjelduse, mis ümbritsevad korratusi või ebaseaduslikke toiminguid.

6.2.2 Leidudest tuleb teatada sobivatele juhtkonna tasemetele, mis on toimingus osalenud tasemest kõrgemal. Kui on osalenud kõik juhtkonna tasemed või kui IS audiitor kahtlustab kõigi tasemete osalemist, tuleks leidudest teatada kõigepealt organisatsiooni juhtimisüksustele, näiteks direktsioonile, usaldusisikutele või auditikomisjonile.

G19 Korratused ja ebaseaduslikud toimingud (jätkub)

6.2.3 Korratuses või ebaseaduslikust toimingust teatamisel peaks IS audiitor kasutama kutsealast otsustusvõimet. IS audiitor peaks arutama leide ning kõigi edasiste sooritatavate protseduuride iseloomu, ajastust ja ulatust juhtkonna sobiva tasemega, mis on vähemalt ühe taseme võrra kõrgemal isikutest, kes näivad olevat asjasse segatud. Sellistel juhtudel on eriti tähtis, et IS audiitor jääks sõltumatuks. Kui IS audiitor otsustab sobivaid isikuid, kellele teatada korratusest või ebaseaduslikust toimingust, peaks ta arvestama kõiki relevantseid asjaolusid, sealhulgas ka võimalust, et asjasse on segatud kõrgem juhtkond.

6.2.4 IS audiitor peaks püüdma hoiduda alarmeerimast isikuid, kes võisid olla segatud korratusse või ebaseaduslikku toimingusse või selles osaleda; see vähendab võimalust, et need isikud võivad hävitada või peita asitõendeid.

6.3 Aruanded kolmandatele pooltele

6.3.1 Hoolimata organisatsiooni kohustusest teatada ebaseaduslikust toimingust või korratusest ei luba IS audiitori konfidentsiaalsuse kohustus organisatsiooni suhtes tal teatada võimalikest või tuvastatud korratustest või ebaseaduslikest toimingutest.

6.3.2 Teatud asjaoludel aga võidakse IS audiitorilt nõuda korratuse või ebaseadusliku toimingu avaldamist. Sellised asjaolud on näiteks

- õigusaktide nõuete järgimine;
- välisaudiitorite taotlused;
- kohtukutse või kohtuotsus;
- rahastava asutuse või riigiasutuse taotlus, riigilt rahalist toetust saavate asutuste auditeerimise nõuete alusel;

6.3.3 Olukordades, kus IS audiitorilt nõutakse võimaliku või tuvastatud korratuse või ebaseadusliku toimingu avaldamist, tuleks tal enne selle nõude täitmist otsida õigusabi.

6.3.4 Mõnedes jurisdiktsioonides võib IS audiitorit kaitsta eriprivileeg. Ka olukordades, kus IS audiitorit kaitseb eriprivileeg, peaks ta enne sedalaadi avaldamist otsima õigusabi ja veenduma, et see privileeg teda tõepoolest kaitseb.

6.3.5 Kui organisatsioon ei avalda teadaolevat korratust või ebaseaduslikku toimingut või nõuab IS audiitorilt selliste leidude varjamist, peaks audiitor otsima õigusabi.

7 JÕUSTUMISKUUPÄEV

7.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. juulil 2002 või pärast seda.

G20 Aruandlus

1 TAUST

1.1 Seos ISACA standarditega

1.1.1 Standard S7 "Aruandlus" määrab: " Pärast auditi lõpuleviimist peaks IS audiitor koostama sobivas vormis aruande. Aruandesse tuleks märkida organisatsioon, eeldatavad saajad ja võimalikud levituskitsendused. Auditi aruanne peaks teatama sooritatud auditi töö käsitlusala, eesmärgid, hõlmatud perioodi, ajastuse ja ulatuse. Aruanne peaks teatama leiud, järeldused ja soovitused ning kahtlused, piirangud või käsitlusala kitsendused, mis IS audiitoril võivad olla auditi suhtes.

1.2 Määratlused

1.2.1 Teema ehk käsitlusobjekt on spetsiifiline teave, mida käsitlevad IS audiitori aruanne ja sellega seotud protseduurid. Ta võib hõlmata näiteks sisemeetmete kavandamist või käitust või vastavust privaatsuse tavadele või standarditele või spetsifitseeritud õigusaktidele.

1.2.2 Tõendusaruande ülesanne on ülesanne, kus IS audiitor uurib kas juhtkonna väiteid mingi teema kohta või otse teemat. IS audiitori aruanne kujutab endast arvamust alljärgnevate hulgast ühe kohta.

- Teema. Need aruanded puudutavad otse teemat, mitte väidet. Teatud olukordades ei saa juhtkond ülesande teema kohta midagi väita. Selline olukord on näiteks siis, kui IT-teenuseid tellitakse kolmandalt poolelt. Tavaliselt ei saa juhtkond midagi väita nende meetmete kohta, mille eest vastutab kolmas pool. Seetõttu käsitleb IS audiitor aruandes otse teemat, mitte väidet.
- Juhtkonna väide juhtimisprotseduuride toimivuse kohta.
- Uurimisaruande ülesanne on selline, kus IS audiitor avaldab arvamust konkreetse teema kohta. Sellised ülesanded võivad hõlmata aruandeid juhtkonna rakendatud meetmete ja nende kasutamise toimivuse kohta.

See suunis on sihitud esimest tüüpi arvamusele. Kui lähtetingimused nõuavad viimaseid arvamuse tüüpe, ei tarvitse aruandluse nõudeid võib-olla rakendada.

1.2.3 Juhtimiseesmärgid on juhtkonna eesmärgid, mida kasutatakse meetmete (juhtimisprotseduuride) väljatöötamise ja rakendamise raamstruktuurina.

1.2.4 Meetmed või juhtimisprotseduurid tähendavad neid poliitikaid ja protseduure, mida rakendatakse mingi nendega seotud juhtimiseesmärgi saavutamiseks.

1.2.5 Juhtimisnõrkus tähendab mingit puudust juhtimisprotseduuri lahenduses või talitluses. Juhtimisnõrkuste tulemuseks võivad olla aktsepteeritavaist suuremad riskid, mis puudutavad käsitlusobjekti (asjassepuutuvad riskid on need, mis ohustavad uuritavat käsitlusobjekti puudutavate eesmärkide saavutamist). Juhtimisnõrkused võivad olla kaalukad, kui ühe või mitme juhtimisprotseduuri lahendus või talitlus ei vähenda suhteliselt madala tasemeni riski, mis ähvardab sellega, et võivad esineda ja jääda vastavate juhtimisprotseduuridega avastamata ebaseaduslikest toimingutest või korratustest põhjustatud vääresitused.

1.2.6 Kriteeriumid on standardid ja mõõtlusalused, mille abil mõõdetakse ja esitatakse käsitlusobjekti ning millega võrreldes hindab IS audiitor käsitlusobjekti. Kriteeriumid peaksid olema

- objektiivsed, st nihkevabad;
- mõõdetavad, st peaksid võimaldama järjekindlat mõõtmist;
- täielikud, st peaksid sisaldama kõiki järelduse tegemiseks asjassepuutuvaid tegureid;
- asjassepuutuvad, st seotud käsitlusobjektiga.

1.2.7 Otsearuande ülesanne on selline ülesanne, kus juhtkond ei esita kirjalikku väidet oma juhtimisprotseduuride toimivuse kohta ning IS audiitor esitab arvamuse otse käsitlusobjekti kohta, näiteks juhtimisprotseduuride toimivuse kohta.

1.2.8 Sisejuhtimisstruktuur (sisejuhtimine) on dünaamiline integreeritud protsesside kogum, mida mõjutavad juhtimisüksus, juhtkond ja muu personal ning mis on mõeldud andma mõistlikku kinnitust järgmiste üldiste eesmärkide saavutamise kohta:

- tegevuse toimivus, tõhusus ja ökonoomsus;
- halduse usaldatavus;
- vastavus kehtivatele õigusaktidele ja sisemistele poliitikatele.

1.2.9 Juhtkonna strateegiaid nende üldeesmärkide saavutamiseks mõjutavad järgmiste komponentide lahendus ja talitlus:

- juhtimiskeskkond,
- infosüsteem,
- juhtimisprotseduurid.

1.3 Suunise vajadus

1.3.1 See suunis näitab, kuidas IS audiitor peaks organisatsiooni infosüsteemide meetmete ja nendega seotud juhtimiseesmärkide käsitlemisel aruandes järgima ISACA infosüsteemide auditeerimise standardeid ja COBITit.

2 SISSEJUHATUS

2.1 Selle suunise eesmärk

2.1.1 Selle suunise eesmärk on anda juhiseid IS audiitoritele, kellele on tehtud ülesandeks teatada, kas spetsifitseeritud käsitlusobjekti juhtimisprotseduurid on toimivad, ühele järgmistest:

- organisatsiooni juhtkonnale, tipp- või tegevtasemel;
- spetsifitseeritud kolmandale poolele, näiteks reguleerivale asutusele või teisele audiitorile.

2.1.2 IS audiitorile võidakse teha ülesandeks teatada lahenduse toimivusest või talitluse toimivusest.

3 KINNITUS

3.1 Teenuste liigid

3.1.1 IS audiitor võib sooritada ühe järgmistest:

- auditi (otsese või tõendite põhjal),
- läbivaatuse (otsese või tõendite põhjal),
- kokkulepitud protseduurid.

3.2 Audit ja läbivaatus

3.2.1 Audit annab tugeva, kuid mitte absoluutse kinnituse juhtimisprotseduuride toimivuse kohta. Harilikult nimetatakse seda mõistlikuks kinnituseks, tunnistades tõsiasja, et absoluutne kinnitus on vaevalt saavutatav selliste tegurite tõttu nagu otsustusvajadus, testimise kasutamine, sisejuhtimise olemuslikud kitsendused ning et suur osa IS audiitorile kättesaadavaist asitõenditest on loomult pigem osutav kui otsustav.

3.2.2 Läbivaatus annab mõõduka kinnituse juhtimisprotseduuride toimivuse kohta. Saadav kinnitus on nõrgem auditiga saadavast, sest töö käsitlusala on kitsam kui auditi puhul ning sooritatavate protseduuride iseloom, ajastus ja ulatus ei anna piisavaid ja sobivaid auditi asitõendeid, mis võimaldaksid IS audiitoril väljendada kindlat arvamust. Läbivaatuse eesmärk on võimaldada IS audiitoril öelda, kas ta on protseduuride põhjal märganud midagi sellist, mis paneks ta arvama, et piiritletud kriteeriumide järgi ei olnud juhtimisprotseduurid toimivad (eitava kinnituse väljendus).

3.2.3 Juhtimisprotseduuride auditid ja läbivaatused sisaldavad

- ülesande plaanimist;
- juhtimisprotseduuride lahenduse toimivuse hindamist;
- juhtimisprotseduuride talitluse toimivuse kontrollimist (kontrollimise iseloom, ajastus ja ulatus on auditi ja läbivaatuse puhul erinev);

- piiritletud kriteeriumide põhjal järelduse kujundamist ja aruandmist juhtimisprotseduuride lahendusliku ja talitlusliku toimivuse kohta:

  - auditi järeldus väljendatakse arvamuse jaatava väljendusena ja annab tugeva kinnituse,

  - läbivaatuse järeldus väljendatakse kinnituse eitava väljendusena ja annab mõõduka kinnituse.

3.3 Kokkulepitud protseduurid

3.3.1 Kokkulepitud protseduuridega ülesanne ei anna tulemuseks mingi kinnituse väljendust IS audiitorilt. IS audiitorile on tehtud ülesandeks sooritada konkreetsed protseduurid, nende protseduuride sooritamises kokkuleppinud osapoolte teabevajaduste rahuldamiseks. IS audiitor esitab aruande tegelike leidude kohta neile osapooltele, kes leppisid kokku protseduuride suhtes. Selle aruande saajad kujundavad aruande põhjal omaenda järeldused, sest IS audiitor ei ole määranud protseduuride iseloomu, ajastust ja ulatust ega saa seetõttu väljendada mingit kinnitust. Aruanne esitatakse ainult neile osapooltele (näiteks regulatiivsele organile), kes leppisid kokku selles, millised protseduurid tuleb sooritada, sest teised ei tea põhjusi nende protseduuride sooritamiseks ja võivad tulemust vääralt tõlgendada.

3.4 Aruandlus kokkulepitud protseduuride kohta

3.4.1 Aruanne kokkulepitud protseduuride kohta peaks vormilt olema protseduuride ja leidude esitus. Aruandes peaksid olema järgmised elemendid:

- pealkiri, mis sisaldab sõna "sõltumatu";
- määratud osapoolte piiritlus;
- käsitlusobjekti (või sellega seotud kirjaliku tõenduse) ja ülesande tüübi piiritlus;
- vastutava osapoole piiritlus;
- lausung selle kohta, et käsitlusobjekt on vastutava poole vastutusel;
- lausung selle kohta, et sooritati need protseduurid, mille suhtes leppisid kokku aruandes piiritletud osapooled;
- lausung selle kohta, et protseduuride piisavuse eest vastutavad täielikult aruandes piiritletud osapooled, ning lahtiütlus vastutusest nende protseduuride piisavuse eest;
- sooritatud protseduuride (või neile suunatud viidete) ja nendega seotud leidude loetelu;
- lausung selle kohta, et IS audiitorile ei tehtud ülesandeks uurida käsitlusobjekti ja et ta ei teinud seda;

- lausung selle kohta, et kui IS audiitor oleks sooritanud lisaprotseduure, oleks ta võib-olla märganud muid asjaolusid ja oleks esitanud need aruandes;
- lausung aruande kasutamise kitsenduste kohta, mis tulenevad sellest, et aruanne oli mõeldud kasutamiseks ainult piiritletud osapooltele.

3.5 Ülesande mandaat

3.5.1 Kui ülesanne tuleb sooritada regulatiivsete või muude selliste sundnõuete täitmiseks, on tähtis, et IS audiitor saaks veenduda, et ülesande tüüp selgub asjassepuutuvast õigusaktist või muust ülesande mandaadi allikast. Igasuguse ebaselguse puhul on soovitatav, et IS audiitor ja/või ülesande andja võtaksid ühendust asjassepuutuva regulatiivse asutusega või muu poolega, kes on kehtestanud nõude või reguleerib seda, ning lepiksid kokku ülesande tüübi ja vajaliku kinnituse suhtes.

3.5.2 Kui IS audiitorilt taotletakse enne ülesande täitmise lõpetamist selle ülesande muutmist auditist ülevaateks või kokkulepitud protseduuridega ülesandeks, peab audiitor kaaluma, kas see sobib, ega saa nõustuda muudatusega, kui muudatuseks ei ole mõistlikku põhjendust. Näiteks ei ole muudatus sobiv, kui ta nõuab aruande muutmist.

4 IS AUDITI ARVAMUS

4.1 Kitsendused

4.1.1 IS audiitori otsus põhineb protseduuridel, mis otsustati olevat vajalikud piisavate ja sobivate asitõendite kogumiseks, kusjuures need asitõendid on pigem osutavad kui otsustavad. IS audiitori antavat kinnitust sisemeetmete toimivuse kohta kitsendavad aga sisemeetmete iseloom ning iga sisemeetmestiku ja ta talitluse olemuslikud kitsendused. Selliste kitsenduste hulka kuuluvad alljärgnevad.

- Juhtkonna tavaline nõue, et sisemeetme hind ei ületaks tema rakendamisest oodatavaid hüvesid.
- Enamik sisemeetmetest on suunatud pigem rutiinsetele kui mitterutiinsetele tehingutele ja sündmustele.
- Hooletusest, tähelepanu hajumisest, väsimusest, juhiste vääritimõistmisest ja otsustusvigadest tingitud inimeksituste võimalus.
- Võimalus sisemeetmetest mööda hiilida töötajatevaheliste või töötajate ja väljaspool organisatsiooni olevate poolte vaheliste salakokkulepetega.
- Võimalus, et mingi sisemeetme rakendamise eest vastutaja võib seda kohustust kuritarvitada; näiteks võib juhtkonna liige juhtimisprotseduurist mööduda.

- Võimalus, et juhtkonnale ei rakendata samu sisemeetmeid, mida rakendatakse teistele töötajatele.
- Tingimuste muutumise tõttu võivad sisemeetmed muutuda puudulikeks ja protseduuride järgimine võib nõrgeneda.

4.1.2 Tavad, kultuur ja halduse (organisatsiooni ja IT) süsteemid võivad takistada juhtkonnapoolseid korratusi, kuid nad ei ole veatud tõrjevahendid. Selliste korratuste tõenäosust võib aidata vähendada toimiv juhtimiskeskkond. Juhtkonna sobimatut käitumist võivad piirata sellised juhtimiskeskkonna tegurid nagu toimiv haldusüksus, auditikomisjon ja siseauditi talitus. Toimimatu juhtimiskeskkond seevastu võib nurjata juhtimisprotseduuride toimivuse sisejuhtimise struktuurides. Näiteks võivad organisatsioonil küll olla adekvaatsed IT juhtimise protseduurid, mis on seotud keskkonda puudutavate õigusaktide järgimisega, kuid juhtkonnal võib olla tugev kalduvus varjata teavet kõigi avastatud rikkumiste kohta, sest see teave mõjuks kahjulikult organisatsiooni välisele kuvandile. Asjassepuutuvate sisemeetmete toimivust võivad mõjutada ka näiteks omanduse või juhtimise muudatus, muudatused juhtkonnas või muus personalis või arengud organisatsiooni turul või tegevusalal.

4.2 Järgnevad sündmused

4.2.1 Pärast käsitlusobjekti kontrollimise hetke või perioodi, kuid enne IS audiitori aruande tähtaega võivad mõnikord leida aset sündmused, millel on kaalukas mõju käsitlusobjektile ning mis seetõttu vajavad korrigeerimist või avaldamist käsitlusobjekti esituses või kinnituses. Selliseid juhtumeid nimetatakse järgnevateks sündmusteks. Kinnitusülesande täitmisel peaks IS audiitor arvestama teavet talle teatavaks saanud järgnevate sündmuste kohta. IS audiitor ei ole aga kohustatud avastama järgnevaid sündmusi.

4.2.2 IS audiitor peaks küsitlema juhtkonda selle kohta, kas juhtkonnale on teada mingid sellised järgnevad sündmused ajavahemikul enne IS audiitori aruande tähtaega, millel võiks olla kaalukas mõju käsitlusobjektile või kinnitusele.

4.3 Järeldused ja aruandlus

4.3.1 IS audiitor peaks läbi vaatama ja hindama hangitud asitõenditest tehtud järeldused, mis on aluseks arvamuse kujundamisele juhtimisprotseduuride toimivuse kohta, piiritletud kriteeriumide põhjal.

4.3.2 IS audiitori aruandes juhtimisprotseduuride toimivuse kohta peaks olema alljärgnev:

- pealkiri;
- adressaat;
- auditi käsitlusala kirjeldus, sealhulgas
- käsitlusobjekti piiritlus või kirjeldus;

G20 Aruandlus (jätkub)

- IS audiitori järelduse aluseks olevad kriteeriumid;
- lausung selle kohta, et sisejuhtimisstruktuuri, sealhulgas käsitlusobjekti juhtimisprotseduuride, toimivuse säilitamine on juhtkonna kohus;
- kui ülesanne on tõendusülesanne, siis lausung, mis teatab juhtkonna esituse allika juhtimisprotseduuride toimivuse kohta;
- lausung selle kohta, et IS audiitor on täitnud ülesande arvamuse väljendamiseks juhtimisprotseduuride toimivuse kohta;
- IS audiitori aruande koostamise eesmärgi ja selle saajate piiritlus ning lahtiütlus vastutusest aruande kasutamise eest mingil muul eesmärgil või muude isikute poolt;
- kriteeriumide kirjeldus või viide nende allikale;
- lausung selle kohta, et audit on läbi viidud vastavalt ISACA infosüsteemide auditeerimise standarditele või muudele kehtivatele kutseala standarditele;
- täiendavad selgitavad üksikasjad saadud kinnitust mõjutavate muutujate kohta ja vajadusel muu teave;
- sobivatel juhtudel peaks eraldi aruanne sisaldama soovitusi parandusmeetmete rakendamiseks ja esitama juhtkonna reaktsiooni;
- lõik, mis teatab, et igasuguse sisejuhtimise olemuslike kitsenduste tõttu võivad vigade või pettuse tõttu leida aset vääresitused, mis võivad jääda avastamata. Peale selle peaks see lõik teatama, et igasuguste rahandusliku aruandluse sisejuhtimise hindamise projektsioonidega tulevastele perioodidele kaasneb risk, et sisejuhtimine võib muutuda puudulikuks, sest tingimused võivad muutuda või poliitikate ja protseduuride järgimine võib nõrgeneda;

  - audit ei ole mõeldud avastama kõiki juhtimisprotseduuride nõrkusi, sest teda ei sooritata pidevalt kogu perioodi kestel ning juhtimisprotseduuride kontrollimised sooritatakse valimite põhjal;

  - kui IS audiitori arvamuses on reservatsioone, tuleks lisada neid kirjeldav lõik;
- arvamuse väljendus selle kohta, kas käsitlusobjekti suhtes oli juhtimisprotseduuride lahendus ja talitlus kõigis olulistes aspektides toimiv;
- IS audiitori allkiri;
- IS audiitori aadress;
- IS audiitori aruande kuupäev. Enamasti põhineb aruande dateerimine kehtivatel kutseala standarditel. Muudel juhtudel peaks aruande dateerimine põhinema välitöö lõpetamisel.

4.3.3 Otsese aruande ülesande korral koostab IS audiitor aruande otse käsitlusobjekti kohta, mitte tõenduse põhjal. Aruanne peaks viitama ainult ülesande käsitlusobjektile ega tohiks sisaldada viiteid juhtkonna väidetele käsitlusobjekti kohta.

G20 Aruandlus (jätkub)

4.3.4 Kui IS audiitor võtab käsile läbivaatuse ülesande, näitab aruanne, et IS audiitori järeldus puudutab lahenduse ja talitluse toimivust ning et talitluse toimivuse puhul piirdub IS audiitori töö eelkõige sisemeetmete talitluse alaste küsitluste, ülevaatuse, vaatluste ja minimaalse testimisega. Aruanne sisaldab lausungi selle kohta, et auditit ei sooritatud, et rakendatud protseduurid annavad nõrgema kinnituse kui audit ja et auditi arvamust ei väljendatud. Eitava kinnituse väljendus ütleb, et IS audiitor ei märganud midagi sellist, mis paneks teda arvama, et organisatsiooni juhtimisprotseduurid oleksid käsitlusobjekti suhtes mingist kaalukast aspektist, piiritletud kriteeriumide põhjal, toimeta.

4.3.5 Ülesande täitmise käigus võivad IS audiitorile saada teatavaiks juhtimisnõrkused. Igast tuvastatud juhtimisnõrkusest peaks IS audiitor aegsasti teatama asjakohasele juhtkonna tasemele. Ülesande protseduurid on kavandatud koguma sobivaid piisavaid asitõendeid järelduse moodustamiseks vastavalt ülesande tingimustele. Kui ülesande tingimustes ei ole sellekohast nõuet, ei ole IS audiitor kohustatud kavandama protseduure selliste asjaolude tuvastamiseks, millest võib-olla tasuks teatada juhtkonnale.

5 JÕUSTUMISKUUPÄEV

5.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. jaanuaril 2003 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary.*

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus

1 TAUST

1.1 Seos ISACA standarditega

1.1.1 ISACA IS auditeerimise standardid ja ka teatavad IS auditeerimise suunised puudutavad otseselt IS audiitori auditi tööd ERP süsteemidega või ERP süsteemide teostamise projektidega.

1.1.2 Näiteks standardi S6 "Auditi töö sooritamine" järgi peab ERP-ga seotud auditi töö, mida sooritab IS audiitori jaoks alluv IS auditi või muu auditi personal, alluma IS audiitori piisavale asjakohasele järelevalvele.

1.1.3 Peale selle peaks IS audiitor sellises olukorras, kus taotletakse või vajatakse tema osalust ERP süsteemi või selle teostusprojektiga seotud auditivälistes rollides, lisaks standardiga S2 "Sõltumatus" ja suunisega G12 "Organisatsiooniline seos ja sõltumatus" seotud IS auditeerimise standarditele ja suunistele vaatama läbi ISACA standardid IS juhtimise spetsialistidele ning asjakohaselt kaaluma nende rakendatavust.

1.1.4 Kui IS audiitoril tuleb auditirolli või auditivälise rolli vaatepunktist osaleda äriprotsessi ümberrajamise (BRP) tegevustes, mis on seotud ERP süsteemi teostamise ja kasutamisega, tuleks läbi vaadata ISACA IS auditeerimise suunis G26 "Äriprotsessi ümberrajamine".

1.1.5 Lisaks ISACA standardinõukogu poolt väljakuulutatuile on (või on olnud) teadusnõukogul rida projekte ja saadusi, mis on kättesaadavad ISACA veebisaidi *(www.isaca.org)* kaudu ja võivad pakkuda huvi IS audiitorile, sõltuvalt sellest, millist konkreetset ERP-toodet ja milliseid muid ressursse kasutatakse.

1.2 Seos COBITiga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- soorituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jäämise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusindikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

1.3 Suunise vajadus

1.3.1 ERP süsteemid, mis arenesid välja töötleva tööstuse tootmisressursside plaanimise süsteemidest, kasutavad mitmesugustest talitlusaladest pärit andmeid mitmeid allüksusi hõlmava juhtimis- ja protsessiteabe loomiseks. Termin ERP tähistab mitte enam ainult plaanimist, vaid organisatsiooni keskseid elutähtsaid äriprotsesse. See kontseptsioon on küll põhimõtteliselt kasulik, kuid ERP süsteemide teostused ei pruugi anda oodatud tulemusi, kui neid adekvaatselt ei hallata ega juhita. Pealegi on tekkimas tendentse ja tehnoloogilisi muutusi, mis toetavad ERP süsteemide laiendatud kasutamist (näiteks veebipõhiseid kliendiliideseid), see aga suurendab ERP puhul turva- ja juhtimiskaalutluste tähtsust.

1.3.2 ERP süsteemi audit nõuab IS audiitorilt eriteadmisi ja konkreetsetesse tarnija toodetesse ehitatud ning nende edukaks evitamiseks, kasutamiseks ja juhtimiseks vajalike keerukate eriomaduste ja integreeritud protsesside tundmist.

1.4 Suunise rakendamine

1.4.1 Selle suunise rakendamisel peaks IS audiitor arvestama ta juhiseid seoses muude asjassepuutuvate ISACA standarditega ja asjassepuutuvate suunistega. Suunis on koostatud andma mitte tootespetsiifilisi, vaid üldistatud juhiseid. IS audiitoril on vaja arvestada ja sobitada neid juhiseid sõltuvalt kasutatavast ERP süsteemist ja muudest kasutatavatest toodetest või protseduuridest.

1.4.2 See suunis esitab teavet ja soovitab, kuidas ERP süsteemi või ta teostusprojekti auditis või läbivaatuses osalev IS audiitor peaks järgima ISACA standardeid ja COBITit.

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

2 ETTEVÕTTE RESSURSSIDE PLAANIMISE (ERP) SÜSTEEMID

2.1 Määratlused

2.1.1 Ettevõtte ressursside plaanimine tähendab eelkõige ettevõtte ressursside plaanimist ja haldust. Teiseks tähistab ta tarkvarasüsteemi, mida saab kasutada kogu ettevõtte protsesside halduseks, integreerides hankimise, laomajanduse, personalihalduse, klienditeeninduse, kohaletoimetuse, rahalise halduse ja ettevõtte tegevuse muud aspektid. Tavaliselt põhineb ERP süsteem ühisel andmebaasil, mitmesugustel integreeritud äriprotsessi rakendusmoodulitel ja tegevuse analüüsi instrumentidel.

2.2 ERP süsteemide rakendamise riskid ja juhtimisprobleemid

2.2.1 ERP süsteeme rakendatakse ettevõtte tegutsemise toetuseks; olemaks edukad, peavad nad olema täielikult integreeritud kõigi oluliste protsesside ja protseduuridega, mis koos võimaldavad ettevõttel töötada toimivalt. Oma integreeritud iseloomu tõttu võivad ERP süsteemid lisada organisatsioonile riske ja probleeme, mis on seotud järgnevaga:

- keskkond tegevusalal ja ettevõtte tegevuses;
- kasutajate või juhtkonna käitumine;
- äriprotsessid ja -protseduurid;
- süsteemide funktsioonid;
- rakenduste turvalisus;
- aluseks olev infrastruktuur;
- andmete konversioon ja terviklus;
- hoolduse ja tegutsemise pidev jätkuvus.

2.2.2 ERP süsteemi rakendamise ja pideva kasutamisega seotud riske ei saa määrata ega ohjata rakenduse või tehniliste riskide eraldi läbivaatusega, vaid neid tuleb arvestada teenindatava organisatsiooni äriprotsesside juhtimiseesmärkidega seostatult. Seetõttu on IS audiitori ülesanne õppida tundma tegevusalast ja regulatiivset keskkonda, milles tegutseb organisatsioon, ning osata tuvastada kvantiteeritavad rakenduste või tehnilised riskid ja vähemkvantiteeritavad protseduuri- või käitumisriskid.

2.2.3 Suurtes organisatsioonides, kus ERP süsteemiga töödeldavate andmete maht on äärmiselt suur, osutub tavaliselt talitluse toimivuse ja tõhususe tõendamisel väga kasulikuks andmemustrite ja tendentside analüüs. Enamik ERP süsteeme annab võimalusi ja eriinstrumente selliseks ekstraheerimiseks ja analüüsiks. ERP süsteemis olevate andmeanalüüsi instrumentide kasutamine võib abistada IS audiitorit kogu ERP elutsükli kestel (st evituseelsel-, aegsel ja järgsel perioodil).

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

2.3 Äriprotsessi ümberrajamine (BPR) ja ERP rakendamine

2.3.1 BRP ja ERP rakendamise projekte võib vaadelda sõltumatute üritustena. Teoreetiliselt võib kumbki neist projektidest eksisteerida organisatsioonis ilma teiseta. Praktikas on nad organisatsioonis sageli mõlemad korraga töös ning mõjutavad üksteist ja sõltuvad üksteisest; sageli on neil kesksete äriprotsesside jaoks ühesugune lahendus. ERP võidakse valida olemasolevat süsteemi asendama, BPRi teostamine võib aga hilineda. BPR võib olla töös, kuid võidakse katkestada enne lõpuleviimist, ERP süsteemi rakendamine võib aga jätkuda.

2.3.2 Sageli on BPR ja ERP teostused väljatöötamise erinevates järkudes. Võidakse alustada BPR-projekti ning mõne kuu pärast jõuda järeldusele, et uute protsesside toetuseks on vajalik ERP, ja käivitada hankeprojekti. Samuti võidakse teha tegevusalane otsus hankida uus IT-süsteem ja valida ERP. Teostusprotsessi käigus võib selguda, et see ERP võimaldab äritegevuse ümberrajamist, ja võidakse alustada BPR-üritust.

2.3.3 IS audiitor peaks keskenduma eelkõige ERP teostusele. Samal ajal toimuv BPR võib aga lisada teostusprotsessile uusi riske ning sageli muuta seniseid riske, näiteks järgmiselt.

- BPR-iga pakutavad muudatused võivad nõuda asjassepuutuvailt teistsugust käitumist ning võivad organisatsioonis kutsuda esile toetust, muretsemist ja/või isegi vaenu. See võib üle kanduda ERP teostamise projekti.
- BPR võib kulutada organisatsiooni ressursse, mis on määratud ERP teostamiseks.
- Ka siis, kui kaks ülalnimetatud riski ei mõjuta ERP teostust, võib teadmatus BPR-iga loodud uute protsesside alal viia protsesside ebaadekvaatse kirjeldamiseni ja ERP mitteoptimaalse konfiguratsioonini.
- BPR ja ERP võivad olla halvasti integreeritud, andes tulemuseks parimal juhul mitteoptimaalse soorituse ja asjatud kulutused.
- ERP kasutamine "muudatuste hoovana" võib juhtida tähelepanu eemale BPR-ilt. Uue võimsama tehnoloogiaga kaasneb kiusatus rakendada mingit protsessi lihtsalt sellepärast, et uus tehnoloogia "saab sellega hakkama", mitte aga sel põhjusel, et see protsess on optimaalne äriprotsess.

2.3.4 Alljärgnevas on tavalised BPR sooritamise sammud; eriti juhitakse tähelepanu neile sammudele, kus IT võib avaldada tugevat mõju.

- Analüüsi järk. Analüüsitakse olemasolevaid protsesse, teavet ja kasutuselolevaid IT-süsteeme ning selgitatakse välja protsessid, mis tuleb ümber rajada. Kuna teabe ja IT kasutamine võivad olla organisatsiooni protsesside järskude muudatuste hoobadeks, saavad IS audiitorid anda kasulikke panuseid BPR-protsessi varajastes järkudes.

- Ümberkavandamise järk. Kavandatakse ümber uued protsessid, otsitakse uut teavet või uusi senise teabe kasutamise viise ning määratletakse uue talitlussüsteemi kavand. IS auditiga kaetavateks aladeks võivad olla uue töövoo sihtmudel, uue teabe ühiskasutuse viisid ettevõtte talituste vahel ning uute IT-süsteemide spetsifikatsioonid.
- Ümberkujunduse järk. Töötatakse välja ülemineku strateegia, koostatakse ülemineku tegevusplaan ja viiakse see ellu. IS auditiga kaetavateks aladeks võivad olla IT-süsteemide ümberkujundamine, uue teabe ja uute tehnoloogiate kasutuselevõtt ning vana teabe ja IT-süsteemide kõrvaldamine.

2.4 COBITi rakendamine ja kasutamine

2.4.1 ERP süsteemide läbivaatamisel saab mitmeti rakendada COBITit. Kuna eri organisatsioonidel on erinevad juhtimisstruktuuride vajadused, erinevad ka nende asjakohased juhtimiseesmärgid. COBITi rakendamist ülevaatuse käigus oleks aga hea alustada ettevõtte komplekslahendusi puudutavate juhtkonna IT-probleemide käsitlemisest (vt COBITi rakendusjuhend). Gartner Group on piiritlenud mõned ERP süsteeme puudutavad konkreetsed juhtkonna probleemid, sealhulgas järgmised:

- kasutaja nõuete täitmata jätmine;
- integreerimata jätmine;
- ühildumatus tehnilise infrastruktuuriga;
- tarnijatoe probleemid;
- kallid ja keerulised installeeringud.

2.4.2 Eelnimetatud probleemide käsitlemiseks võib kasutada ISACA piiritletud asjassepuutuvaid juhtimiseesmärke. Peale selle võib IS audiitor visandada ülesandespetsiifilised juhtimiseesmärgid ja ülesandespetsiifilised auditeerimisprotseduurid nende konkreetsete juhtimiseesmärkide puhuks.

3 TOIMIV IS AUDITEERIMISE STANDARDITE JÄRGIMINE

3.1 Sissejuhatavaid kommentaare

3.1.1 IS audiitori algsel kokkupuutumisel ERP süsteemiga või ERP süsteemi teostamise projektiga või selles mingi rolli täitmisel on väga asjakohased ISACA IS auditeerimise standardid ja IS auditeerimise suunised ning IS audiitor peaks neid arvestama ja asjakohaselt järgima. IS audiitorile tuleks suuresti kasuks nende auditeerimisstandardite ja -suuniste põhjalik läbivaatus ja analüüs ERP süsteemi ja sellega seotud ürituste puhuks kavandatud rolli või töö kontekstis.

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

3.1.2 Selle suunise otstarbel viidatakse konkreetselt ainult teatavatele asjakohasematele IS auditeerimise suunistele. ERP süsteemid annavad IS audiitoritele mitmesuguseid võimalusi ning tekitavad juhtkonnale riske, mida tuleb käsitleda hoolikuse ja plaanimisega. ERP süsteemi plaanimisjärk või teostuse läbivaatus on eluliselt tähtis edukaks auditiks ja üleandmiseks.

3.1.3 ERP süsteemi või teostuse audit nõuab IS audiitorilt teistsugust strateegilist lähenemist. ERP süsteemid integreerivad mitmesuguseid äriprotsesse ning seetõttu võidakse neid teostada seoses BPR-projekti läbiviimisega. Sellise ümberrajamise ühe osana võidakse asendada või kõrvaldada elutähtsaid juhtimisprotseduure, millega varem kaitsti organisatsiooni rahalisi varasid ja talitlust, nii et tulemuseks saadakse täiesti uued juhtimisstruktuurid ja -protseduurid ning nendega kaasnevad riskid.

3.1.4 ERP süsteemide või teostusprojektide puhul peaks IS audiitor ümber rajama ka auditite sooritamise viisi. Muutuvad riskide intensiivsus, liigid ja riskide võimaliku realiseerumise teed. Teatud määral tekivad need riskid ERP tarkvaratoodetele omase integreeritud programmiloogika ja talitlusprotsesside funktsioonistiku tõttu. Peale selle ei saa paljusid pärandmeetmeid enam rakendada ning IS audiitoril tuleb sellisel juhul piiritleda uus juhtimisstruktuur.

3.1.5 ERP süsteemi IS-auditi plaanimisel peaks IS audiitor tõsiselt kaaluma auditi jaotamist lõikudeks ja lõikude järjestikku auditeerimist, sest kogu ERP audit on suur ettevõtmine ning võib kurnata IS-ressursse või muid auditi ressursse.

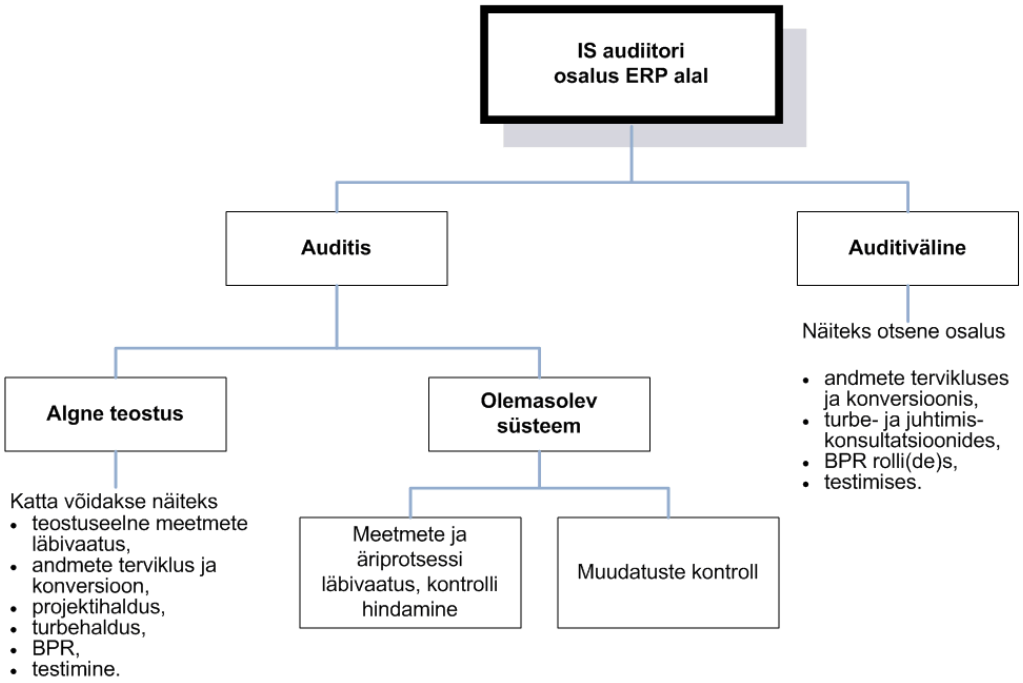
3.2 Auditi põhikiri

3.2.1 Kui organisatsioon on otsustanud teostada ERP süsteemi, tuleb võib-olla muuta IS auditeerimise talituse põhikirja. Näiteks võivad ERP süsteemi toimiva rakendamisega seotud BPR-kaalutlused nõuda, et IS audiitori töö käsitlusala või seoseid teiste audititalitustega (näiteks rahandusliku või tegevusalasega) laiendataks ja tihedamalt integreeritaks (näiteks ühise või koostöise auditiüritusena).

3.2.2 IS audiitori sooritatava auditi plaaniline käsitlusala tuleks määratleda vastavalt IS auditi talituse põhikirjale.

3.2.3. On möödapääsmatu, et organisatsiooni kõrgem ja süsteemijuhtkond täielikult tunneks ja toetaks IS audiitori rolli (rolle) ERP süsteemi või teostusprojekti alal. Tuleks läbi vaadata IS auditeerimise suunis G5 "Audititalituse põhikiri" ja arvestada seda organisatsiooni ERP ja sellega seotud ürituste kontekstis.

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)



3.3 Sõltumatus

3.3.1 Kui IS audiitoril tuleb täita ERP süsteemiga või ERP süsteemi teostusprojektiga seotud auditiväliseid rolle või nende eest vastutada, tuleks läbi vaadata IS auditeerimise suunis G17 "Auditivälise rolli mõju IS audiitori sõltumatusele" ja seda asjakohaselt järgida.

3.3.2 Kui IS audiitoril tuleb täita ERP süsteemis või sellega seotud üritustes auditivälist rolli, peaks ta läbi vaatama ISACA IS juhtimise kutsealased standardid ja neid asjakohaselt järgima.

3.4 Pädevus

3.4.1 IS audiitori pikatähtajalised auditi strateegiad ja plaanid ERP süsteeme kasutava organisatsiooni kohta peaksid sisaldama aspekte, mis toetavad IS auditi pidevat arendust ja hooldust ning IS audiitori pädevust ERP alal. Need hõlmavad oskuste ja teadmiste tasemetõusu ja pidevat kutsealast õpet (standard S4).

3.4.2 Kui IS audiitoril ei ole ERP süsteemi või teostusprojekti IS auditi ettevõtmiseks vajalikke oskusi, peaks ta kaaluma selle auditi väljasttellimist kvalifitseeritud IS audiitorilt. Lepingusse tasuks võtta teadmiste edastuse nõude.

3.4.3 ERP süsteemi teostuse auditeerimise oskusi võib omandada ERP auditeerimis- või tootekoolituse läbimisega, töökogemuste saamisega ning ERP aladel või auditirühmades osalemisega.

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

3.4.4 Konkreetse tootega seotud (näiteks võib konkreetsete ERP toodete puhul olla terminoloogia teistsugune või teistsuguse tähendusega) koolitust ja kogemusi võib saada praktilise kasutamisega ning küsitluse või vaatlusega. Konkreetse ERP süsteemi turbe, juhtimise ja töötluse erijooni või riske võivad IS audiitoril aidata tundma õppida taustausutlused või süsteemi eest vastutavalt IS juhtkonnalt, tehniliselt personalilt ja kasutajaskonnalt saadav teavitus.

3.4.5 Lisajuhiseid pädevuse lünkade kõrvaldamise kohta annab selle suunise lisa.

3.5 Plaanimine

3.5.1 ERP süsteemi või teostusprojekti IS auditi alustamisel peaks IS audiitor pühendama piisavalt aega ja tööd taustateabe kogumisele ning ettekujutuse saamisele organisatsiooni olemasolevast ja plaanilisest ERP süsteemi ja sellega seotud ressursside rakendamisest ja kontrolli alla saamisest. IS audiitor saavutab selle tooteuuringuga, juhtkonna ja muu personali otsese küsitlemisega ning dokumentide läbivaatuse protseduuridega.

3.5.2 Lisa annab konkreetsema üldise ülevaate ERP süsteemi teostuse elementide ja põhiliste sellega seotud küsimuste kohta, mida IS audiitoril tuleb võib-olla arvestada.

3.5.3 ERP süsteemid ja teostused on küll tõenäoliselt integreeritumad ja keerukamad muudest talitlussüsteemidest, millega IS audiitor võib olla kokku puutunud, kuid nad sisaldavad palju selliseid organisatsiooni halduse, keskkonna, rakenduste ja juhtimise kaalutlusi ja riske, mis sarnanevad traditsioonilisemate süsteemide ja teostusprojektide omadele.

3.5.4 Eriti tuleb pöörata tähelepanu sellele, et need alad, kus IS audiitor võiks osaleda ERP projekti auditi käigus, kataksid ettevõtte tegevuse kõiki aspekte. Seetõttu nõuab ERP süsteemi täielik audit väga laialdasi oskusi, mida tõenäoliselt ei ole ühel isikul või ühes auditeerimisdistsipliinis. On eluliselt tähtis, et ERP auditiläbivaatuses osaleks õige auditeerimisoskuste spekter. IS audiitori oskusi on võib-olla vaja täiendada rahanduse, talitluse ja reguleerimise alade auditioskuste ja -ressurssidega.

3.5.5 Plaanimise ajal on tähtis mõelda sellele, kas ja millised ERP protsessid ulatuvad veebi. Kuna paljude organisatsioonide tegevus ulatub ettevõtteportaalide ja uutel mobiilse andmetöötluse vahenditel olevate veebipõhiste rakenduste kaudu veebi, peaks IS audiitor tegema kindlaks, kas auditeerida tulev ERP kuulub sellesse liiki (st kasutab sisevõrku, partnerivõrku või Internetti). See võib mõjutada audititöö sooritamist ja võib laiendada ERP piire.

3.5.6 IS audiitorid peaksid saama mõistliku kinnituse sellele, et juhtkond on teadlik sooritamisele kuuluva audititöö käsitlusalast ja on sellega rahul.

3.6 Töö sooritamine

3.6.1 IS audiitor võib ERP keskkonna auditeerimiseks kasutada mitmesuguseid vahendeid ja meetodeid, millega käsitleda terveid populatsioone, märgistada võimalikke riske ja sooritada läbivaatus toimivalt. ERP süsteemi algselt kavandatud

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

meetmed nõrgenevad sageli mingi aja pärast. Pealegi on tekkimas keskkond, kus ERP on mitte ainult liidestatud muude süsteemidega, vaid võib olla ka veebipõhiseks keskkonnaks, kus protsesside piirid ulatuvad väljapoole ERP süsteemi ennast ning on ilmne, et tuleb mõelda vahenditele ja meetoditele alljärgneva tarbeks.

- Andmete kaevandamine ja analüüs. Harilikult kuuluvad ERP toodete juurde stabiilsed auditiga seotud aruanded; kui neid ei ole, võib elutähtsate andmete või valimite väljaselgitamiseks ja analüüsimiseks kasutada kolmandate poolte instrumente.
- Kohustuste lahususe analüüs ja volituste analüüs. Teave ei ole suletud eraldiseisvaisse allüksuste süsteemidesse; ERP süsteemi integreeritud iseloomu tulemuseks on suured riskid turvalisuse ja pääsuõiguste alal. Talitlusreeglite analüüsi abil saab välja selgitada juhud, kus märgistada läbivaatuseks võimalikud turvaprobleemid.
- Töövoog ja aruannete väljastus. Töövoogu ERP süsteemides saab kasutada erandiaruannete väljastuseks võtmeisikutele analüüsimiseks ja läbivaatuseks. Kuna teave on kättesaadav reaalajas, on algpõhjuste analüüs palju lihtsam ja on võimalik algatada talitluslikke parandusmeetmeid.
- Ajakohastuste ja juhtimise arukad vahendid. ERP toodete tarnijad jätkavad investeerimist uurimis- ja arendustöösse, mis viib uute või täiustatud funktsioonideni, rääkimata juba olemasolevate funktsioonide pidevast parandamisest. Organisatsioonile, sealhulgas IS audiitorile, on oluline olla kursis ERP uusimate funktsioonide, suutvuse halduse ja juhtimisvõimalustega. On olemas instrumendid, millega ajakohastada tehnilisi juhtimissätteid, mis on kasutusel ERP süsteemis, nii algses teostuses kui ka täiendversioonis.

3.6.2 ERP audit võib anda kinnituse, mis katab protsessitervikluse ala. Kaaluda tuleks järgmisi konkreetseid samme.

- Välja selgitada teostamisel olevate protsesside juhtimiseesmärgid.
- Tuvastada ja kaalutleda teostamisel olevate protsesside võimalikud tegevusriskid ja rahalised riskid.
- Töötada välja ja kavandada kõige toimivad ja tõhusamad moodused nende riskide ohjeks (teostajad ei pööra üldiselt sellele tähelepanu või puudub neil kogemus nende mooduste väljatöötamiseks).
- Sooritada kesksete põhitegevuste sõltumatu analüüs, võrreldes organisatsiooni protsesse juhtivate tavadega ja soovitades protsesside täiustusi.
- Saada kinnitus sellele, et meetmed ERP süsteemis on sobivad ja toimivad.
- Vaadata läbi muudest süsteemidest (näiteks pärilussüsteemidest, veebipõhistest ja mobiilse andmetöötluse rakendustest) ERP-süsteemi sisenevad liidesed.

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

- Sooritada auditikontrollid, keskendudes äriprotsessidele ja sisejuhtimisele.
- Vaadata läbi tegutsemise jätkusuutlikkuse plaanid ja saada mõistlik kinnitus sellele, et neid on testitud.

3.6.3 ERP audit võib anda kinnituse, mis katab rakenduste turvalisuse ala. Kaaluda tuleks järgmisi konkreetseid samme.

- Vaadata läbi tüüpsed ERP parameetrid, sealhulgas rakenduste meetmed, volitused ja tüüpne turbekonfiguratsioon. Hinnata rakenduste turvet, mis peaks kaitsma hinnalisi andmeid, kuid ühtlasi võimaldama tõhusat ja juhitavat töötlust.
- Hinnata konfigureerimisotsuseid; see aitab saada mõistlikku kinnitust äriprotsesside tervikluse ja rakenduste turvalisuse kohta.
- Vaadata läbi projekteerimisdokumentatsioon sobiva turvalisuse ja juhtimise seisukohalt.
- Hinnata turbe administreerimise protsessi, taotledes kinnitust sellele, et pääsuõigused on asjakohaselt piiritletud, hinnatud ja kinnitatud.
- Paljud äriprotsessid võivad ulatuda sisevõrku, partnerivõrku või Internetti. IS audiitor peaks taotlema mõistlikku kinnitust sellele, et turbeprotsessid käsitlevad asjakohaselt sellega kaasnevaid riske.

3.6.4 ERP audit võib anda kinnituse, mis katab infrastruktuuri tervikluse ala. Kaaluda tuleks järgmisi konkreetseid samme.

- Selgitada välja rakendustarkvara paketti toetava infrastruktuuri (st riistvara, operatsioonisüsteemi, andmebaasihalduse tarkvara, võrguaparatuuri, Interneti ja sisevõrgu) võimalikud konfiguratsiooni- ja turvariskid
- Läbi vaadata organisatsiooni IT infrastruktuuri võime toetada organisatsiooni tavasid ja tulevasi tegevussihte.
- Selgitada välja sisemise süsteemiarhitektuuri aspektid, mis võivad põhjustada sooritusvõime, käideldavuse või andmetervikluse probleeme.
- Vaadata läbi tegutsemise jätkusuutlikkuse plaanid ja saada mõistlik kinnitus sellele, et neid on testitud.

3.6.5 ERP audit võib anda kinnituse, mis katab teostuse tervikluse ala. Kaaluda tuleks järgmisi konkreetseid samme.

- Saada mõistlik kinnitus sellele, et uude ERP keskkonda siirdutakse sujuvalt, töötajaid minimaalselt mõjutades ning kaotamata usaldust andmete tervikluse, turvalisuse ja täpsuse suhtes.
- Tuvastada võimalikud riskid, mis on seotud andmete üleviimisega pärilussüsteemidest uude tootmiskeskkonda ning liidestega ERP ja teiste süsteemide vahel.
- Enne käikuandmist testida ja hinnata funktsioone, juhtimisvahendeid ja valmidust.

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

- Hinnata andmete kvaliteeti.
- Hinnata andmete konversiooni ja tervikluse strateegiaid ja juhtimisprotseduure.
- Hinnata testimisplaani (-plaane) täielikkuse ning sobivat turvalisuse ja tervikluse seisukohalt.
- Saada kinnitus sellele, et testimine on kaasanud kavatsetud kasutajaskonda ja et uue ERP omanik on rahul täieliku kasutajatepoolse aktsepteerimisega.
- Sooritada koolituse sõltumatu läbivaatus äriprotsessi täielikkuse ja turvakaalutluste seisukohalt.
- Sooritada teostusjärgne juhtimis- ja turvakeskkonna toimivuse ning teostusprotsessi üldise halduse läbivaatus.
- Hinnata eranditest teatamist.

3.6.6 ERP teostuse auditeerimise võib läbi viia projekti elutsükli suvalisel hetkel, auditeerides seda, mis on selleks hetkeks tehtud ja seda, mis on plaanitud edaspidiseks. Ideaaljuhul sisaldaks audit läbivaatust pidevana või projekti elutsükli mitmes punktis. Selleks vajab IS audiitor auditi raamstruktuuri, mis hõlmab teostuse kõige olulisemaid alasid, kus sageli peituvad suured riskid. Niisugused alad on näiteks

- projektihaldus,
- kvaliteedihaldus,
- hüvede haldus,
- riskihaldus,
- muutusehaldus.

3.6.7 Projektihaldus koosneb neljast järgust; need on alljärgnevad.

- Halduse plaanimine. Projekti algatamisel koostatakse halduse plaan, lepitakse kokku pakutavate hüvede suhtes ning määratletakse projekti käsitlusala ja struktuur.
- Projekti teostamine. Kogu projekti kestel sooritatakse keskseid projektihalduse tegevusi: töö plaanimist, ressursihaldust, projekti juhtimist, projekti aruandlust ja teavitamist.
- Projekti lõpetamine. Projektil peaks olema ettemääratletud ja kergesti tuvastatav lõpp-punkt, kus ERP süsteem siirdub teostusjärgust tegelikku käitusesse.
- Hüvede tekitamine. Pärast teostusjärku muutub projektihalduse iseloom ja haldus siirdub äriprotsessi omanikule, kelle kohus on tagada, et kasutajate käitumises tekivad vajalikud muudatused ja et saadakse hüvesid.

3.6.8 ERP süsteemi projektihaldus ei erine oluliselt ega põhjapanevalt ükskõik millise muu suure tarkvaraprojekti haldusest. Samad kontseptsioonid kehtivad ka ERP süsteemi teostuse halduse auditi puhul, näiteks järgmiselt.

- Sooritada juhtide ja tippjuhtkonna toe hindamine.
- Sooritada projektihalduse tegevuste sõltumatu läbivaatus ja analüüs.

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

- Hinnata sõltumatult projekti plaanimist ja juhtimist ning kvaliteedi tagamist.
- Esitada juhtkonnale leiud, mis puudutavad projektiprobleemide lahendamist, sealhulgas tähtaegade või eelarve ületused, lüngad funktsioonides ning lahknevused personali- ja kvalifikatsiooninõuetest, samuti muud projektihaldust puudutavad probleemid.

3.6.9 Kvaliteedihaldus, mis peaks olema kõigi tarkvaraprojektide lahutamatu osa, peaks tegelema mitte ainult projekti tarneobjektidega, vaid hõlmama kõiki ERP projekti tegevusi ja saadusi, näiteks projekti plaanimist, kavandamisedokumentatsiooni, spetsifikatsioone, protseduure, koolitusmaterjale ja teostusplaane. Kvaliteedi tagamist, mida tuleks projekti organisatsiooni sees sooritada sõltumatu funktsioonina, ei tuleks lugeda auditeerimistegevuseks. Teisalt on väga oluline auditeerida ERP süsteemi teostamise käigus kvaliteedihalduse ja kvaliteedi tagamise toimivust.

3.6.10 Hüvede halduse auditi jaoks on huvikeskmeteks äriplaan ja sellega seotud plaan hüvede realiseerumise kohta. Nad peaksid piiritlema alljärgneva.

- Projekti ärieesmärgid ja eeldatavad saavutatavad hüved. Hüved (nii kvantitatiivsed kui ka kvalitatiivsed) tuleks selgelt spetsifitseerida hüvede registris. Kvantiteeritud hüved tuleks liigendada tuvastatavaiks ja mõõdetavaiks elementideks.
- Hüvede realiseerumise plaanimine ning nende seos äriprotsesside muutusehaldusega.
- Juhtimisprotseduurid, millega saadakse mõistlik kinnitus hüvede saavutamisele.

3.6.11 Hüvede halduse audit, mis viiakse läbi enne ERP süsteemi teostamise algust, on võimeline andma edukale ERP projektile olulisi hüvesid. Hüvede realiseerumise audit tuleks läbi viia mingi aja (tavaliselt 18 kuu) möödumisel projekti lõpetamisest.

3.6.12 Riskihaldus ei ole pelgalt projekti riskide haldus, ta hõlmab ka nende riskide haldust, mida ERP projekt võib tuua kaasa äritegevusele. IS audiitor peaks tegelema mitmesugust tüüpi riskide haldusega:

- riskihaldusega, mis puudutab ümberrajamisele kuuluvaid äriprotsesse;
- riskihaldusega, mis on seotud projektihaldusega; projekti riskid võivad olla

  - olemuslikud, mis tulenevad projekti eesmärkide ja käsitlusala iseloomust; või

  - omandatud, mis tulenevad projekti- ja riskihaldusele rakendamiseks valitud metoodikatest, vahenditest, meetoditest, oskustest ja kogemustest;
- infoturbe haldusega süsteemi teostamise ajal;

- infoturbe haldusega, mis on plaanitud süsteemi käikuandmisele järgnevaks ajaks, st süsteemi käituse puhuks;
- selliste riskide haldusega, mida tekitavad ERP projekti suhtes välised süsteemid, ja selliste riskide haldusega, mida ERP projekt võib tekitada kolmandatele pooltele. Seega peaks IS audiitor käsitlema ettevõtet laiemalt, mitte keskenduma kitsalt ühele konkreetsele ERP projektile.

3.6.13 Eduka projektihalduse jaoks väga olulised tegevused on organisatsiooni ümberkorraldamine, teavitus, projekti turundamine ja personali koolitamine. Lisaks ülalnimetatud tegevustele peaks IS audiitor hindama ka muutusehalduse seost muude elutähtsate teostusaladega, eriti hüvede haldusega (taotletavate hüvede seisukohalt) ja riskihaldusega (mis puudutab võimalikku vastupanu muudatusele ja infoturvet, mis on seotud isikute õigustega nende ümbermääratletud rollides). Harilikult nõuab ERP teostamisest hüvede tulenemine seda, et enne teostust kavandataks uued protsessid rakenduse funktsioonide loomiseks ning et pärast teostust kasutajad muudaksid oma käitumist nii, et see sobiks uute kavandatud protsessidega. Seega jätkub ärihüvede tulenemise audit pärast traditsioonilise ERP projekti sulgemist.

3.7 Aruandlus

3.7.1 Aruandluse protsessid auditi arvamuse teatamiseks ja/või auditi kommentaaride andmiseks ERP projekti kohta ei erine olemuslikult ükskõik millistest muudest auditi aruandluse protsessidest. Sobida võivad mõned või kõik järgmistest aruandluse mehhanismidest:

- regulaarsed kokkuvõttearuanded ERP projektihalduse koosolekutele või korralduskomisjoni koosolekutele (võib-olla päevakorrapunktidena);
- projekti päeviku pidamine selgitamist vajavate auditiküsimuste või lahendamist vajavate juhtimisprobleemide jälgimiseks;
- formaalsed aruanded auditi arvamusega ja lahendamata küsimustega, projekti elutsükli ettemääratud järkudes.

4 JÕUSTUMISKUUPÄEV

4.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. augustil 2003 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

LISA

Toetumine COBITile

Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ja arvestades COBITi teabekriteeriume.

See suunis on kavandatud nii, et oleks välditud ta rakendamise piiramine ERP mingi kindla liigiga. Ta on kavandatud katma kõiki ERP kasutamise aspekte organisatsioonis. Seetõttu saab selle suunise siduda COBITi kõigi nelja alaga: plaanimise ja organiseerimise, hankimise ja evituse, tarnimise ja toe ning seire ja hindamisega.

Kui mingit konkreetset auditiprojekti peaks ta auditi põhikiri piirama konkreetse ERP ühe aspektiga konkreetses majandusüksuses, on kohaldatavad COBITi alad ja äriprotsessid muidugi vastavalt piiratud. Selle illustreerimiseks on järgnevas kaks näidet. Nad ei ole mõeldud ammendavatena ning konkreetne auditi käsitlusala võib põhjendatult muuta seda, millised protsessid tuleks valida.

Näide 1:

ERP plaanimise ja hankimise audit või läbivaatus

Plaanimine ja organiseerimine

- PO1 – Määratleda strateegiline IT plaan
- PO2 – Määratleda infoarhitektuur
- PO3 – Määratleda tehnoloogiline suund
- PO4 – Määratleda IT protsessid, organisatsioon ja seosed
- PO5 – Hallata IT-investeeringuid
- PO6 – Teavitada juhtimissihid ja suund
- PO7 – Hallata IT inimressursse
- PO8 – Tagada vastavus välisnõuetele (COBIT v3)
- PO9 – Hinnata IT riskid ja hallata neid
- PO10 – Hallata projekte
- PO11 – Hallata kvaliteeti (COBIT v3)

Hankimine ja evitamine

- HE1 – Tuvastada automatiseeritud lahendused
- HE2 – Hankida rakendustarkvara ja hooldada seda

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE4 – Võimaldada käitus ja kasutamine

Näide 2:

küpse ERP süsteemi audit või läbivaatus

Plaanimine ja organiseerimine

- PO4 – Määratleda IT protsessid, organisatsioon ja seosed
- PO5 – Hallata IT-investeeringuid
- PO7 – Hallata IT inimressursse
- PO8 – Tagada vastavus välisnõuetele (COBIT v3)
- PO9 – Hinnata IT riskid (COBIT v3)
- PO11 – Hallata kvaliteeti (COBIT v3)

Hankimine ja evitamine

- HE2 – Hankida rakendustarkvara ja hooldada seda
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE4 – Võimaldada käitus ja kasutamine
- HE6 – Hallata muutusi

Tarnimine ja tugi

- TT1 – Määratleda teenusetasemed ja hallata neid
- TT2 – Hallata kolmandate osapoolte teenuseid
- TT3 – Hallata suutlikkust ja võimsust
- TT4 – Tagada pidev teenus
- TT5 – Tagada süsteemide turvalisus
- TT6 – Tuvastada ja kinnistada kulud
- TT7 – Koolitada kasutajaid
- TT8 – Hallata konsultatsioonipunkti ja intsidente
- TT9 – Hallata konfiguratsiooni
- TT10 – Hallata probleeme
- TT11 – Hallata andmeid
- TT12 – Hallata füüsilist keskkonda
- TT13 – Hallata käitust

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

Seire ja hindamine

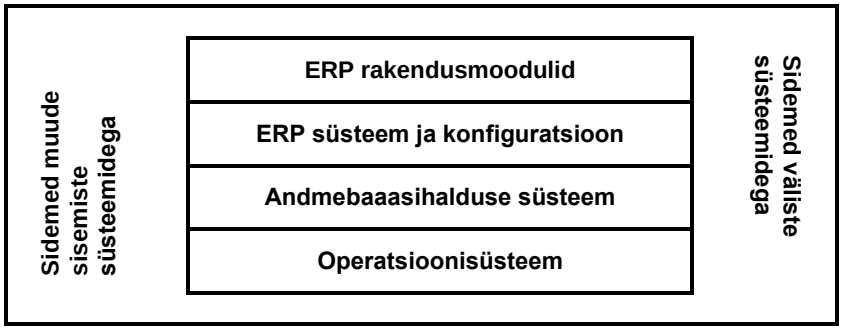
- S1 – Seirata protsesse (COBIT v3)
- S2 – Hinnata sisejuhtimise adekvaatsust (COBIT v3)
- S3 – Saada sõltumatu kinnitus (COBIT v3)
- S4 – Korraldada sõltumatu audit (COBIT v3)

ERP teadmuse- ja oskusenõuded

	ERP süsteem	Teostusprojekt
IS audiitori taust-teadmised	Rahanduslike ja halduslike meetmete ja juhtimisriskide üldine tundmine IS auditeerimise kutsealaste standardite rakendamise põhjalik tundmine IT-ga seotud meetmete ja juhtimisriskide põhjalik tundmine järgmistel aladel: • IT keskkond • rakendused / töötlus Klient-server-arhitektuuri tundmine Operatsioonisüsteemide ja andmebaasihalduse süsteemide tundmine ERP-de ning nende kavandamise ja rakendamise põhimõtete (sealhulgas nende mõju kontrolljälgedele) üldine tundmine ERP moodulite ning nende konfigureerimis-, integreerimis- ja rakendamisviiside tundmine Turvalisuse ja volitamise kontseptsioonide tundmine ERP kontekstis	Üldiste projektihalduse tavade ja meetmete tundmine Projektihalduse tavade ja meetmete tundmine IT alal IT-ga seotud süsteemi-arenduse metoodikate ja standardite tundmine, sealhulgas muutusehalduse alal Äriprotsesside ümberrajamise põhimõtete ja nende rakendamise tundmine
IS audiitori oskused	Kogenud IS auditeerimise professionaal, kes on võimeline keskenduma juhtimisriski otsustavatele aladele ERP kontekstis Arvutipõhiste auditeerimismeetodite (CAAT) ja nende rakendamisviiside tundmine ERP kontekstis Võimelisus tuvastada, kus on vaja täiendavaid oskusi või kogemusi (näiteks rahanduse või regulatsiooni alal)	Teostusprojektide läbivaatuse ja hindamise kogemus
Kuidas omandada oskusi	Sertifitseerimine kutselise audiitorina Sertifitseerimine kutselise IS audiitorina, näiteks CISA Spetsialistide kursused, mis keskenduvad nii ERP-de haldusele ja kasutamisele kui ka ERP-de auditile ERP tundmaõppimise võimalused, eriti lõppkasutajaskonna liikmena Töökohal saadav praktiline kogemus Iseõppimine, uurimistöö, Internet jms	Osalemine spetsialistide kursustel, mis keskenduvad ERP teostusprojektidele ja IS audiitori rollile sellistes projektides Töökohal saadav praktiline kogemus Iseõppimine, uurimistöö, Internet jms

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

ERP süsteemi teostuse üldised elemendid



Küsimused ERP süsteemi teostamise kohta

- Millist ERP-toodet ja milliseid mooduleid kasutatakse praegu või edaspidi?

  - Kuidas on need moodulid omavahel seotud (näiteks andmevood läbi moodulite)?

- Milliseid andmebaasihalduse tooteid kasutatakse praegu või edaspidi?

  - Kuidas on ERP praegu või edaspidi konfigureeritud andmebaasihalduse süsteemiga?

- Milliseid operatsioonisüsteemitooteid kasutatakse praegu või edaspidi?

  - Kuidas igaüht neist konfigureeritakse/rakendatakse ja ohjatakse?

- Millise tasemeni on ERP veebipõhine?

  - Millised protsessid ulatuvad veebi?

- Millised on liidesed või sidemed organisatsioonisiseste või -väliste ERP-väliste süsteemidega praegu või edaspidi?

- Kuidas juhitakse iga funktsiooni praegu või edaspidi?

- Millises ulatuses on ERP funktsioonid ja juhtimisrollid või -kohustused praegu või edaspidi tsentraliseeritud või detsentraliseeritud?

- Kuidas ohjas ja testis või ohjab ja testib juhtkond andmeterviklust vanadest ERP süsteemidest või ERP-välistest süsteemidest pärit andmete konverteerimisel ERP teostamise käigus?

- Millises ulatuses toimus või toimub ERP teostusprojekti käigus äriprotsesside ümberrajamine?

  - Kui ei toimu(nud), siis miks? Millal see toimub?

- Kui see toimus/toimub, siis millised muudatused tehakse ja miks?

- Kuidas lepivad ERP ja BPR projektid kokku ühiste protsessikavandite suhtes?

- Milliseid IT riistvara- ja võrguressursse kasutatakse praegu ja edaspidi ning kuidas neid konfigureeritakse ja hallatakse?

G21 Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus (jätkub)

- Millises ulatuses on ERP halduse ja tehnilise toe rollid ja kohustused integreeritud muu asjassepuutuva IT toega (näiteks andmebaasi administreerimisega, käitusega)?
- Milliseid meetmeid rakendatakse alljärgnevate komponentide muutusehalduse protsessidele?

  - ERP rakendusmoodulid,

  - ERP tuumsüsteem,

  - andmebaasihaldus,

  - operatsioonisüsteem,

  - BPR muudatused,

  - muud ERP-väliste süsteemidega ühendavad sidemed või liidesed.
- Millised on praegu või edaspidi juurdepääsu turbe poliitikad ja standardid ning kelle vastutusel on juhtkonna pidev kontroll ja tugi?
- Milliseid protsesse kasutatakse mõistliku kinnituse saamiseks sellele, et ERP süsteemi vastuvõtmine ja omanduse üleandmine kasutajate juhtkonnale on lõpule viidud?

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.2 Juhiseid annab suunis G14 "Rakendussüsteemide läbivaatus".

1.1.3 Juhiseid annab suunis G16 "Kolmandate poolte mõju organisatsiooni IT-meetmetele"

1.1.4 Juhiseid annab suunis G17 "Auditivälise rolli mõju IS audiitori sõltumatusele".

1.2 Seos COBITiga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- soorituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jäämise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusse indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

1.3 Suunise vajadus

1.3.1 Selle suunise eesmärk on kirjeldada ettevõtte ja kliendi vahelise (B2C) e-äri ürituste ja rakenduste läbivaatuseks soovitatavaid tavasid, nii et läbivaatuse käigus järgitaks asjasse puutuvaid IS auditeerimise standardeid.

2 B2C E-ÄRI

2.1 Määratlus

2.1.1 Terminit "e-äri" kasutatakse eri kohtades erinevates tähendustes. ISACA määratleb e-äri kui protsesse, millega organisatsioonid viivad läbi äritegevust oma klientide, tarnijate ja muude väliste äripartneritega elektrooniliselt, kasutades võimaldava tehnoloogiana Internetti. Seega hõlmab see termin nii ettevõtetevahelise (B2B) kui ka ettevõtte ja kliendi vahelise (B2C) e-äri mudeleid, kuid ei hõlma Interneti-väliseid e-äri meetodeid (nagu seda on EDI ja SWIFT), mis põhinevad privaatvõrkudel.

2.1.2 Selle suunise otstarbeks kasutatakse ISACA e-äri määratlust alusena B2C tüüpi e-äri järgmise määratluse saamiseks: B2C tüüpi e-äri tähendab protsesse, millega organisatsioonid viivad läbi äritegevust oma klientidega ja/või üldsusega, kasutades võimaldava tehnoloogiana Internetti.

2.2 E-äri B2C-mudelid

2.2.1 Üha suurem arv organisatsioone kujundab oma tegevust ümber, kasutades B2C-suhetes Interneti tehnoloogiat. Millises ulatuses kasutatakse organisatsioonis B2C-suhetes Interneti tehnoloogiat, sõltub organisatsiooni suhtelisest Interneti-küpsusest, ta klientidest, Interneti kasutamisest ta geograafilisel turustusalal, organisatsiooni toodete ja teenuste iseloomust ning suhtelisest pakilisusest kasutada Internetti konkurentsieeliste saamiseks või konkurentsis püsimiseks. Vastavalt sellele võib organisatsioon võtta abiks e-äri mingi B2C-mudeli, mis hõlmab üht või mitut järgmistest üldistest e-äri tegevustest.

- Teavitus (avalik). Organisatsiooni ja ta tooteid puudutava teabe tegemine Internetis kättesaadavaks kõigile, kes soovivad saada juurdepääsu sellele teabele.
- Kliendi selve (teabeline). Tooteid, teenuseid, hindu jms puudutava teabe tegemine Internetis kättesaadavaks organisatsiooni klientidele.

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

- Kliendi selve (tehinguline, mittemakseline). Lisaks teabe kättesaadavaks tegemisele Internetis võimaldatakse kliendile tehinguid (näiteks tellimist ja tellimuste tühistamist) Interneti kaudu, kuid makseid käsitletakse traditsiooniliste vahenditega.
- Kliendi selve (maksed). Kliendile võimaldatakse tehinguid Interneti kaudu, sealhulgas makseid või ülekandeid (pankade puhul).
- Aruandlus klientidele. Klientidele väljastatakse võrgu kaudu aruandeid, näiteks kontoseise ja tellimuste olekut.
- Interaktiivne selve. Meili teel interaktiivsete vastuste andmine veebisaitide kaudu saadud päringutele.
- Otsemüük. Toodete ja teenuste otsene müümine eeldatavaile ostjaile Interneti kaudu.
- Oksjon. Toodete oksjonmüük võrgu kaudu.

2.3 Erilist tähelepanu nõudvad aspektid B2C-tüüpi e-äri läbivaatusel

2.3.1 B2C-tüüpi e-äri ürituste puhul on äritegevus ja infosüsteem väga tihedalt seotud. Seetõttu peaks B2C-tüüpi e-äri läbivaatus üldiselt käsitlema nii äririske kui ka IS riske.

2.3.2 COBIT sõnastab seitse teabekriteeriumi, millele peavad vastama infosüsteemid. Parem vastavus aitab leevendada IS riske ja aitab vähendada äririske. Need kriteeriumid on

- toimivus,
- tõhusus,
- konfidentsiaalsus,
- terviklus,
- käideldavus,
- vastavus,
- usaldatavus.

Sõltuvalt sellest, millises ulatuses sooritab organisatsioon üldisi e-äri tegevusi (mis on spetsifitseeritud jaotises 2.2.1), võivad need kriteeriumid olla rohkem (igal juhul mitte vähem) asjakohased B2C tüüpi e-äri puhul. Seetõttu peaks B2C tüüpi e-äri läbivaatus käsitlema seda, kuidas B2C tüüpi e-äri rakendus rahuldab COBITi teabekriteeriume ja kuidas leevendatakse temaga seotud riske.

2.3.3 Kuna B2C tüüpi e-äri rakendused on ühendatud Internetiga, ähvardavad neid olemuslikud välised ohud (näiteks häkkerid, viirused, teesklus), mis võivad mõjutada B2C tüüpi e-äri rakenduse konfidentsiaalsust, terviklust ja käideldavust. Kui selline rakendus on integreeritud tagasüsteemidega, on olemas ka nende süsteemide mõjutamise risk.

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

Kui organisatsiooni e-äri B2C-rakendusele toimivad sellised ründed, võivad nad tõsiselt kahjustada organisatsiooni mainet ja imagot. Selles kontekstis peaksid läbivaatused pöörama suurt tähelepanu selliste ohtude eest kaitsmise adekvaatsusele.

2.3.4 B2C tüüpi e-äri oluline nõue on tehingute eitamise vääramine. Üks COBITi seitsmest teabekriteeriumist on terviklus. Tehinguid ja/või makseid sisaldava B2C tüüpi e-äri puhul tuleb suhtluse ajal tagada allika autentsus ja teabe terviklus, nii et tehingut ei saaks hiljem salata. B2C tüüpi e-äri läbivaatus peaks sellistel juhtudel käsitlema B2C tüüpi e-äri rakenduse toimivust salgamise vääramisel.

2.3.5 Üldiselt kaasneb B2C tüüpi e-äriga üksikasjade hankimine e-äri B2C-rakendusi kasutavate ja/või nende kaudu tehinguid tegevate klientide ja kliendikandidaatide kohta. Tuleb tagada selliste üksikasjade privaatsus. See tähendab, et kogutud üksikasju tuleks kasutada ainult kavatsetud eesmärkidel ning vastavalt kokkuleppele isikutega, kes seda teavet annavad. Eri maades on kujunenud mitmesugused õigusnormid. Selles kontekstis peaks iga B2C tüüpi e-äri läbivaatus käsitlema vastavust asjassepuutuvate maade õigusnormidele ning privaatsust puudutavatele parimatele tavadele.

2.3.6 Kuna B2C tüüpi e-äri puhul puuduvad tehingute ja maksete tõendid paberil, on rakenduste kontrolljälgedel selles keskkonnas suurem tähtsus. Selles kontekstis peaks B2C tüüpi e-äri läbivaatus käsitlema kontrolljälgede ja nende läbivaatuse protsesside adekvaatsust. See on tähtis tehingute autentsusele ja terviklusele (sealhulgas ka salgamise vääramisele) kinnituse saamise seisukohalt.

2.3.7 Muude äritegevuskanalitega võrreldes sõltub B2C tüüpi e-äri tugevalt rakenduse käideldavusest ja pääsusu Internetti. Selles kontekstis peaksid nii süsteemi kui ka sidekanali jaoks olemas loodud asjakohased suutvuse plaanimise protsessid, liiasused ja tagasivõtuvõimalused ning avariijärgse taaste protseduurid. B2C tüüpi e-äri käideldavusaspektide hindamisel tuleks sellele pöörata vajalikku tähelepanu.

2.3.8 Üks tähtis aspekt on andmete terviklus B2C tüüpi e-äri rakenduse ning sellega seotud tagarakenduste ja -protsesside (sealhulgas käsiprotsesside, näiteks maksete mitte-elektrooonilise väljastuse ja vastuvõtu) vahel. Sellist terviklust tagama mõeldud rakenduse- ja käsiprotsessimeetmete adekvaatsus peaks olema B2C tüüpi e-äri läbivaatuse oluline osa.

2.3.9 Kui B2C tüüpi e-äri sisaldab maksete saamist võrgu kaudu, peaksid olema kasutusel asjakohased protsessid maksete volitamiseks ja nende nõutava vastuvõtu tagamiseks. Sellistel juhtudel tuleb B2C tüüpi e-äri läbivaatuse osana hinnata meetmete sobivust ja adekvaatsust.

2.3.10 Üsna tihti sisaldab B2C tüüpi e-äri kolmandatest pooltest tarnijate kasutamist mitmesuguste aspektide tarbeks, näiteks rakenduste väljatöötamiseks ja hoolduseks, veebisaidi ja sellega seotud andmebaaside haldamiseks. Sellistel juhtudel tuleb B2C tüüpi e-äri läbivaatuse osana hinnata niisuguste meetmete ja lepinguliste kaitseabinõude sobivust ja adekvaatsust, mis tagavad asjakohased teenusetasemed ning organisatsionni ja ta kliente puudutava teabe kaitse.

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

3 PÕHIKIRI

3.1 Volitused

3.1.1 Enne B2C tüüpi e-äri läbivaatuse alustamist peaks IS audiitor saama mõistliku kinnituse sellele, et tal on sellise kavandatud läbivaatuse sooritamiseks vajalikud volitused IS audiitori positsiooni tõttu või organisatsioonilt saadud kirjalike volituste näol. Kui läbivaatuse algatas organisatsioon, peaks IS audiitor saama mõistliku kinnituse ka sellele, et organisatsioonil on läbivaatuse sooritamiseks vajalikud õigused.

4 SÕLTUMATUS

4.1 Kutsealane objektiivsus

4.1.1 Enne ülesande vastuvõtmist peaks IS audiitor andma mõistliku kinnituse sellele, et tema võimalikud huvid läbivaadatava B2C tüüpi e-äri suhtes ei kahjusta mitte mingil viisil läbivaatuse objektiivsust. Võimaliku huvide vastuolu korral tuleks sellest organisatsioonile selgelt teatada ning enne ülesande vastuvõtmist tuleks organisatsioonilt saada kirjalik lausung selle kohta, et organisatsioon on vastuolust teadlik.

4.1.2 Kui IS audiitoril on või on olnud mingeid auditiväliseid rolle läbivaadatavas B2C tüüpi e-äri rakenduses, peaks ta arvestama suunist G17 "Auditivälise rolli mõju IS audiitori sõltumatusele".

5 PÄDEVUS

5.1 Oskused ja teadmised

5.1.1 IS audiitor peaks andma mõistliku kinnituse selle kohta, et tal on B2C tüüpi e-äri rakenduse läbivaatuseks vajalikud ärialased teadmised. B2C tüüpi e-äri rakenduste või ürituste hindamiseks on tähtis tunda äritegevust, mida toetab B2C tüüpi e-äri rakendus.

5.1.2 IS audiitor peaks andma mõistliku kinnituse ka sellele, et on olemas juurdepääs B2C tüüpi e-äri rakenduse läbivaatuseks asjassepuutuvatele tehnilistele oskustele ja teadmistele. Niisugused läbivaatused nõuavad tehnilisi teadmisi selliste aspektide hindamiseks, mis hõlmavad kasutatavat krüpteerimistehnoloogiat, võrguturbe arhitektuuri ning selliseid turbetehnoloogiaid nagu tulemüürid, sissetungi tuvastamine ja viirusetõrje. IS audiitoril peaksid olema adekvaatsed teadmised nende aspektide läbivaatuseks. Kui osutuvad vajalikeks asjatundjate teadmised, tuleks asjakohast teavet hankida välistelt eriala asjatundjatelt. Väliste asjatundjate kasutamise faktist tuleks organisatsioonile kirjalikult teatada.

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

6 PLAANIMINE

6.1 Riski kaalutlemine üldtasemel

6.1.1 IS audiitor peaks koguma teavet, mis puudutab tegevusala üldiselt (sest B2C tüüpi e-äri riskid varieeruvad sõltuvalt tegevusalast), organisatsiooni eesmärke B2C tüüpi e-äri alal, strateegiat nende eesmärkide saavutamiseks, B2C tüüpi e-äri käsitlusala, süsteemi kasutamise ulatust ning B2C tüüpi e-äri lahenduse loomiseks kasutatavat arendusprotsessi. Seega peaks kogutud teave aitama sooritada äririskide ning COBITi teabekriteeriumidega ja käesoleva dokumendi jaotises 2.3 mainitud aspektidega seotud riskide kaalutlemist üldtasemel. Niisugune riskide kaalutlemine üldtasemel aitab määrata läbivaatuse käsitlusala ja katvust.

6.2 Läbivaatuse käsitlusala ja eesmärgid

6.2.1 IS audiitor peaks selgelt määratlema B2C tüüpi e-äri läbivaatuse käsitlusala ja eesmärgi, vajaduse korral pidades nõu organisatsiooniga. Käsitlusala osana tuleks selgelt sõnastada läbivaatusega kaetavad aspektid. Jaotises 6.1.1 mainitud riski kaalutlemine üldtasemel dikteerib selle, millised aspektid on vaja läbi vaadata, ning läbivaatuse ulatuse ja sügavuse.

6.2.2 Läbivaatuse otstarbeks tuleks välja selgitada ja organisatsiooniga kokku leppida ka lahenduse huvipooled.

6.3 Metoodika

6.3.1 IS audiitor peaks sõnastama metoodika, millega saavutada läbivaatuse käsitlusala ja eesmärgid objektiivselt ja professionaalselt. Järgitav metoodika sõltub sellest, kas läbivaatus on teostuseelne või teostusjärgne. Metoodika tuleks asjakohaselt dokumenteerida. Metoodika ühe osana tuleks spetsifitseerida ka see, kas ja kus kasutatakse välistelt asjatundjatelt saadavat teavet.

6.4 Plaani kinnitamine

6.4.1 Kui see on organisatsioonis tavaks, võib IS audiitor hankida organisatsioonilt plaani ja metoodika kohta nõusoleku.

7 B2C TÜÜPI E-ÄRI LÄBIVAATUSE SOORITAMINE

7.1 Üldist

7.1.1 See jaotis käsitleb nende aspektide laia spektrit, millele tuleb pöörata tähelepanu B2C tüüpi e-äri läbivaatuse sooritamise ajal. B2C tüüpi e-äri konkreetse läbivaatuse tarbeks tuleks selles aspektide laias spektris sõltuvalt läbivaatuse kavandatud käsitlusalast ja eesmärkidest piiritleda läbivaatuse jaoks asjassepuutuvad aspektid.

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

7.1.2 B2C tüüpi e-äri läbivaatus tuleks sooritada määratletu metoodika järgi (vajaduse korral seda detailiseerides), nii et läbivaatuse kavandatud eesmärgid saavutatakse.

7.1.3 Üldiselt tuleks andmete kogumiseks, analüüsimiseks ja tõlgendamiseks sobivalt kasutada olemasoleva dokumentatsiooni (st äriplaani, süsteemi dokumentatsiooni, lepingute, teenusetasemelepete ja logide) uurimist, vestlusi huvipooltega, B2C tüüpi e-äri rakenduse kasutamist ja vaatlemist. Võimaluse korral peaks IS audiitor testima olulisi protsesse testimis- ja/või töökeskkonnas, kontrollides, kas protsessid toimivad nii, nagu on kavatsetud (st testida hankeid või tellimist e-äri süsteemi abil ning testida turvamehhanisme läbistustestimise abil).

7.1.4 Andmete kogumisel, analüüsimisel ja tõlgendamisel võib vajaduse korral kokkuleppel organisatsiooniga sobivalt kasutada teavet välistelt asjatundjatelt.

7.1.5 Järeldused ja soovitused peaksid põhinema nende andmete objektiivsel analüüsil ja tõlgendusel.

7.1.6 Kogutud andmete, tehtud analüüside, tuletatud järelduste ja soovitatavate parandusmeetmete kohta tuleks säilitada asjakohased kontrolljäljed.

7.2 Äriaspektide hindamine

7.2.1 IS audiitor peaks kriitiliselt hindama e-äri eesmärke, strateegiat ja ärimudelit. Organisatsiooni äritegevuse suhtelise positsiooni hindamisel tuleks arvestada ka praegust ja tekkivat konkurentsi. See on oluline eesmärkide ja strateegiate sobivuse hindamiseks ning B2C tüüpi e-äri rakenduse toimivuse ja tõhususe hindamiseks nende eesmärkide ja strateegiate seisukohalt.

7.2.2 IS audiitor peaks välja selgitama, kas B2C tüüpi e-äri üritus on omaette uus äritegevus või on see senise äritegevuse üks lisakanal, ning hindama, mil määral sõltub organisatsiooni edu ja rahaline eluvõime läbivaadatavast B2C tüüpi e-äri üritusest. Mida suurem on sõltuvus B2C tüüpi e-ärist, seda suurem on riskide toime nende materialiseerumise korral.

7.2.3 IS audiitor peaks läbi vaatama äriplaani ja tegema kindlaks, kas B2C tüüpi e-äri kulud ja tulud on kajastatud objektiivselt. Arvestades Interneti kasutajate tohutut ja üha kasvavat arvu projekteeritakse vahetevahel äritegevuse potentsiaal ja mahud tunduvalt kõrgemale pragmaatiliselt saavutatavast tasemest. Kui IS audiitoril on kahtlusi aluseks võetud eelduste kohta, peaks ta nende kohta taotlema selgitusi asjakohaselt juhtkonnalt.

7.3 Detailne riski kaalutlemine

7.3.1 Kui B2C tüüpi e-äri rakendusega seotud olulised protsessid (rakendust ümbritsevad automatiseeritud ja käsiprotsessid) ei ole kergesti kättesaadavad, peaks IS audiitor nad kaardistama.

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

7.3.2 Seejärel peaks IS audiitor kaalutlema neisse protsessidesse puutuvaid tõenäolisi riske (nii äririske kui ka IS riske) ja nende tõenäolist toimet ning dokumenteerima nad koos aspektidega, mis leevendavad või võivad leevendada neid riske. Kaalutleda tuleks ka jääkriski kriitilisust.

7.3.3 Sõltuvalt nende riskide kriitilisusest peaks IS audiitor määrama aspektid, mis tuleb veel läbi vaadata, ja läbivaatuse sügavuse.

7.4 Arendusprotsess

7.4.1 IS audiitor peaks läbi vaatama järgitud arendusprotsessi ja tegema kindlaks, kas B2C tüüpi e-äri rakendusse ehitati sobivad turvamehhanismid.

7.4.2 B2C tüüpi e-äri rakenduse arendus- või hooldusrühma võimed ja kasutatavad instrumendid tuleks läbi vaadata nende adekvaatsuse hindamiseks ja veendumiseks, et B2C tüüpi e-äri rakenduses on sobivad turvameetmed.

7.4.3 Selles kontekstis peaks IS audiitor arvestama suunist G23 "Süsteemi arengu elutsükli (SDLC) läbivaatused", sooritatava läbivaatuse jaoks sobivas ulatuses.

7.5 Muudatuste halduse protsess

7.5.1 Reguleerimata muudatused B2C tüüpi e-äri rakenduses võivad tekitada plaanimata seisakuid ning mõjutada andmete ja töötluse terviklust. Selles kontekstis peaks IS audiitor läbi vaatama muudatuste halduse protsessi sobivuse ja hindama selle adekvaatsust B2C tüüpi e-äri rakenduse keskkonna reguleeritud muudatuste tagamisel. Selle käigus peaks IS audiitor läbi vaatama muudatuste logid ja tegelikud tekitatud muudatused ning kontrollima, kas protsessid toimivad nii, nagu on mõeldud.

7.5.2 IS audiitor peaks kontrollima, kas arenduse, testimise, valmenduse ja käituse keskkonnad on muudatustest tekkivate riskide minimeerimiseks adekvaatselt eraldatud. On vaja hinnata selle aspekti kõigi ebaadekvaatsuste toimeid.

7.6 Sisuhalduse protsess

7.6.1 B2C tüüpi e-äri veebisaitides esitatav sisu (nii ainult teavet andev kui ka tehingutega seotud) tuleks avaldada reguleeritud sisuhalduse protsessiga, mis peab tagama keelelise ja esitusliku sobivuse, teabe õigsuse, avaldatavate andmete asjakohased kinnitused (eriti nende andmete puhul, mis on seotud toodete, teenuste ja tingimustega). IS audiitor peaks läbi vaatama selles protsessis sisalduvad meetmed ja nende järgimise.

7.6.2 IS audiitor peaks kontrollima, kas andmete tervikluse ja õigsuse tagamiseks hoitakse käigus ja vaadatakse läbi adekvaatseid kontrolljälgi olulise sisu (st tingimuste ja hindade) kohta.

7.6.3 Kinnituse saamiseks sellele, et on pööratud adekvaatset tähelepanu õigusnormide järgimisele ja lepingulisele kaitsele, peaks IS audiitor kontrollima, kas B2C tüüpi e-äri rakenduse kasutamise tingimusi ja saidis avaldatud organisatsiooni privaatsuspoliitikaid on uurinud juristid.

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

7.7 Identifitseerimine ja autentimine

7.7.1 Sõltuvalt sellest, milliseid e-äri tegevusi võimaldab B2C tüüpi e-äri rakendus (eriti aga tehingute ja maksete korral), tuleks kasutaja üheselt identifitseerida ja autentida salgamise välistamiseks ja konfidentsiaalsuse säilitamiseks. IS audiitor peaks otsustama, kas identifitseerimiseks ja autentimiseks rakendatavad meetmed, mehhanismid ja tehnoloogiad (näiteks identifikaatorid ja paroolid, digitaalsed sertifikaadid ja digitaalallkirjad) on õiges proportsioonis B2C tüüpi e-äri rakenduse kavatsetud kasutamisega.

7.8 Andmete valideerimine ja maksete volitamine

7.8.1 Kui B2C tüüpi e-äri rakendus võtab tehingute ja/või teabe otstarbel kasutajailt vastu andmeid, peaks IS audiitor kontrollima, kas rakendusse on ehitatud adekvaatsed valideerimisvahendid, mis tagavad sisestatavate andmete sobivuse, ja kas sellised valideerimised toimuvad.

7.8.2 Kui B2C tüüpi e-äri rakendus võimaldab elektroonilisi makseid (näiteks krediitkaardiga), peaks IS audiitor kontrollima, kas maksete autentsuse ja tegeliku laekumise tagamiseks on kasutusel adekvaatsed valideerimise ja maksete volitamise protsessid.

7.9 Side turvameetmed

7.9.1 Kui B2C tüüpi e-äri rakendused töötlevad tehinguid ja makseid ning saavad ja/või esitavad mingeid konfidentsiaalse iseloomuga isikuandmeid (näiteks kontoseise), peaks IS audiitor kontrollima, kas kasutaja ja rakenduse vahelise edastuse krüpteerimiseks on kasutusel sobiv krüpteerimistehnoloogia või -mehhanism (näiteks SSL või IPSec).

7.9.2 Võimaluse ja vajaduse korral peaks IS audiitor kontrollima, kas võrgu kaudu toimuv side on turvatud virtuaalse privaatvõrguga (VPN) ja selle juurde kuuluva krüpteerimisega.

7.10 Töötluse turvameetmed

7.10.1 Kui B2C tüüpi e-äri rakendused töötlevad tehinguid ja makseid, peaks IS audiitor kontrollima, kas töötluse tervikluse ja õigsuse tagamiseks on kasutusel adekvaatsed rakenduste turvameetmed.

7.11 Integratsioon tagaprotsesside ja -rakendustega

7.11.1 Mõned B2C tüüpi e-äri rakendused vajavad tellimuste täitmiseks, raha vastuvõtuks ja tehingute arvelduseks tagaprotsesse. Osa sellest võidakse küll käsitleda eraldi rakendustega või käsiprotsessidega, kuid võib ilmneda vajadus integreerida B2C tüüpi e-äri rakendus mõnede muude rakendustega. Sellistel juhtudel peaks IS

audiitor kontrollima, kas algsete andmete tervikluse kindlustamiseks niisuguste omavahel seotud rakenduste ja protsesside (sealhulgas käsiprotsesside) läbimisel on kasutusel piisavad meetmed, sealhulgas ühitusprotsessid.

7.12 Andmetalletuse terviklus

7.12.1 Iga B2C tüüpi e-äri rakenduse taga on andmebaas, mille terviklus on elutähtis. IS audiitor peaks hindama selle andmebaasi turvameetmeid, kontrollides, kas kasutusel on adekvaatsed mehhanismid andmete sihiliku või tahtmatu kahjustamise, hävitamise või muutmise vältimiseks. Selles kontekstis peaks IS audiitor läbi vaatama selle andmebaasi pääsuõigused ja pääsulogid.

7.12.2 IS audiitor peaks ka läbi vaatama arhiveeritud andmete turvameetmed mõistliku kinnituse saamiseks sellele, et konfidentsiaalsus ja terviklus on adekvaatselt kaitstud.

7.13 Kontrolljäljed ja nende läbivaatus

7.13.1 Nagu eespool mainitud, on automatiseeritud kontrolljälgede roll paber-kontrolljälgede puudumise korral B2C tüüpi e-äri rakenduses elutähtis. IS audiitor peaks läbi vaatama tehingute, sealhulgas maksete, elutähtsates püsiandmetes (näiteks määrad, hinnad, toimingud) toimunud muudatuste ja kõigi süsteemiadministraatori õigustega tehtud muudatuste kontrolljälgede adekvaatsuse.

7.13.2 Kontrolljälgede pelgast olemasolust ei piisa. Kasutusel peaksid olema kontrolljälgede läbivaatuse protsessid, millega anda mõistlik kinnitus sellele, et kontrolljälgedes kajastatud toimingud on õiged ja on asjakohaselt volitatud. Selles kontekstis peaks IS audiitor otsima auditi asitõendeid selle kohta, et kontrolljälgi vaadatakse läbi ja et nende põhjal tegutsetakse.

7.14 Kaitse väliste IS-ohtude eest

7.14.1 IS audiitor peaks hindama väliseid IS-ohte B2C tüüpi e-äri keskkonnale, arvestades organisatsiooni äritegevuse iseloomu. Käsitletavad välised ohud peaksid hõlmama teenusetõkestust, lubamatut juurdepääsu andmetele ja lubamatut arvutiseadmete kasutamist. Neid ohte võivad tekitada mitmesugused allikad (näiteks juhuslikud häkkerid, konkurendid, teiste riikide valitsused, terroristid). Niisuguste ohtude võimalike allikate määramiseks tuleks kasutada organisatsiooni äritegevuse tunnuslikke omadusi (näiteks konkurentsi intensiivsust, turuosa, tehnoloogia kasutamise iseloomu, ajastust ja ulatust ning innovatiivseid või strateegilisi tooteid ja/või teenuseid). Nende ohtudega kaasnev tõenäoline kahju on tihedalt seotud äritegevuse sõltuvusega e-äri protsessidest.

7.14.2 IS audiitor peaks hindama välisohtude tõrjeks kasutatavate kaitsemeetmete võrreldavust kaalutletud riskitasemega. Selles protsessis tuleks IS audiitoril vaadata läbi alljärgnev:

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

- rakenduse tehniline arhitektuur, sealhulgas protokollide valik;
- rakenduse turbe arhitektuur;
- viirusetõrje mehhanism;
- tulemüüri teostus: tulemüürilahenduse sobivus, tulemüüri asukoht, tulemüüripoliitikad, ühendused tulemüüriga ja tulemüürist mööduvad välisühendused;
- sissetungi tuvastuse mehhanismid;
- asjassepuutuvate logide olemasolu ja logide pidev läbivaatus pädeva personaliga;
- rakendatavad protsessid, millega kontrollida vastavust kavandatud arhitektuuridele, poliitikatele ja protseduuridele.

7.15 Vastavus privaatsust puudutavatele õigusnormidele ja parimatele tavadele

7.15.1 IS audiitor peaks hindama, kas organisatsioon järgib asjassepuutuvaid privaatsust puudutavate seadustega ja parimatest tavadega kehtestatud privaatsusnõudeid. Nagu eespool on mainitud, peaks IS audiitor kontrollima, kas privaatsuspoliitikaid ja -tavasid esitatakse asjakohaselt veebisaidis.

7.16 B2C tüüpi e-äri rakenduse käideldavus ja äritegevuse jätkusuutlikkus

7.16.1 Kuna B2C tüüpi e-äri sõltub tugevalt rakenduse käideldavusest ja pääsust Internetti, peaks IS audiitor välja selgitama, kas on kasutusel asjakohased süsteemi ja sidekanali suutvuse plaanimise protsessid, liiasused ja taandumise võimalused, talletus teises asukohas, infokandjate rotatsioon ning avariijärgse taaste protseduurid.

7.16.2 Asjassepuutuvatel juhtudel peaks IS audiitor läbi vaatama taandumise korralduse ning sellega seotud automatiseeritud ja käsiprotsessid, et otsustada nende sobivust äritegevuse jätkusuutlikkuse ja kiire taaste tagamiseks kõigi katkestuste puhul.

7.17 Toimivus ja tõhusus

7.17.1 IS audiitor peaks hindama B2C tüüpi e-äri rakenduse toimivust ja tõhusust, toetudes selle ettevõtmise kavatsetud eesmärkidele. Süsteemi toimivust aitavad hinnata teatud aspektid, näiteks tehingute maht, ettevõtte väärtus, huvitatud klientide, kliendikandidaatide ja külastajate arv, korduvklientide tehingute maht ja väärtus ning klientide kaotamine.

7.17.2 Asjassepuutuvatel juhtudel peaks IS audiitor võrdlema tegelikke ja nägemuslikke kulusid ja tulusid, et otsustada, kas B2C tüüpi e-äri rakendus on piisavalt kuluefektiivne. B2C tüüpi e-äri rakenduse tõhusust aitavad hinnata ka töötlusjõudlus, tagasiside kasutajatelt ja rakenduse kasutamise hõlpsus (mida näitab süsteemi kasutamine).

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

7.17.3 IS audiitor peaks välja selgitama, kas kasutusel on sobivad mehhanismid B2C tüüpi e-äri toimivuse ja tõhususe pidevaks seireks. See peaks hõlmama erandite avastamise ja neist teatamise protsesse vigade ja pettuste vältimiseks.

7.18 Kolmandate poolte teenused

7.18.1 Kui B2C tüüpi e-äri lahendus sõltub kolmandapoolsetest teenuseandjatest, näiteks Interneti-teenuse andjast (ISP), sertifitseerimisorganist (CA), registreerimisorganist (RA) ja veebimajutuse asutusest, peaks IS audiitor tegema kindlaks, kas turbeprotseduurid nende poolel on sobivad ja adekvaatsed.

7.18.2 Selliste kolmandapoolsete teenuseandjate kasutamise puhul peaks IS audiitor läbi vaatama sellega seotud lepingud ja teenusetasemelepped (SLA) ning teenusetasemearuandluse, et otsustada, kas organisatsiooni huve kaitstakse adekvaatselt.

7.18.3 Selles kontekstis peaks IS audiitor mõtlema, kas suunis G16 "Kolmandate poolte mõju organisatsiooni IT-meetmetele" annab sobivaid juhiseid.

7.18.4 Kui B2C tüüpi e-äris kasutatakse kolmandaid pooli sertifitseerimiseks, peaks IS audiitor olema väga hoolikas, kui ta vaatab läbi seda, kuidas kogutakse ja kasutatakse teavet niisuguste kontrollpitserite (BetterBusiness, Webtrust jt) tarbeks.

7.19 Salgamise vääramine

7.19.1 Kui B2C tüüpi e-äri lahendus sisaldab tehingute ja maksete töötlust, peaks IS audiitor hindama asjassepuutuvaid turvameetmeid, mida on nimetatud eespool (jaotistes 7.7, 7.9 ja 7.10) seoses autentimisega, sidega, töötlusega ja salgamise vääramisega.

8 ARUANDLUS

8.1 Aruande sisu

8.1.1 B2C tüüpi e-äri läbivaatuse aruanne peaks sõltuvalt kaetavast käsitlusalast kirjeldama järgmisi aspekte:

- käsitlusala, eesmärk, järgitud metoodika ja eeldused;
- üldine hinnang lahendusele, esitades selle tugevad ja nõrgad küljed ning nõrkade külgede tõenäolise toime;
- soovitused oluliste nõrkuste kõrvaldamiseks ja lahenduse täiustamiseks;
- COBITi teabekriteeriumidele ja B2C tüüpi e-äri spetsiifilistele kriteeriumidele (näiteks salgamise vääramisele) vastavuse ulatus ning kõigi lahknevuste toime;
- soovitused selle kohta, kuidas võiks saadud kogemusi kasutada analoogiliste tulevaste lahenduste või ürituste täiustamiseks.

8.1.2 Enne aruande viimistlemist tuleks leidudele ja soovitustele vajaduse korral saada kinnitus huvipooltelt ja organisatsioonilt.

G22 Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus (jätkub)

9 JÕUSTUMISKUUPÄEV

9.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. augustil 2003 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

LISA

Toetumine COBITile

Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ja arvestades COBITi teabekriteeriume.

B2C tüüpi e-äri ja IT-põhiste äritegevuste puhul on asjakohased kõik IT-protsessid, mis puudutavad plaanimist ja organiseerimist, hankimist ja evitust, tarnimist ja tuge ning seiret ja hindamist.

- PO1 – Määratleda strateegiline IT plaan
- PO2 – Määratleda infoarhitektuur
- PO3 – Määratleda tehnoloogiline suund
- PO8 – Tagada vastavus välisnõuetele (COBIT v3)
- PO9 – Hinnata riskid (COBIT v3)
- HE2 – Hankida rakendustarkvara ja hooldada seda
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE4 – Võimaldada käitus ja kasutamine
- HE5 – Hankida IT-ressursid
- HE6 – Hallata muutusi
- TT1 – Määratleda teenusetasemed ja hallata neid
- TT2 – Hallata kolmandate osapoolte teenuseid
- TT3 – Hallata suutlikkust ja võimsust

B2C tüüpi e-äri auditi seisukohalt kõige asjakohasemad teabekriteeriumid on

- eelkõige: käideldavus, vastavus, konfidentsiaalsus, toimivus ja terviklus;
- teises järjekorras: tõhusus ja usaldatavus.

Allikad

E-äri turvalisuse sarja publikatsioonid. Infosüsteemide Auditi ja Juhtimise Fond (ISACF). 200-2002.

Auditeerimise suunis AGS1056. E-äri. Auditiriski hinnangud ja juhtimiskaalutlused. Austraalia Raamatupidamisuuringute Fond.

G23 Süsteemi arengu elutsükli (SAE) läbivaatused

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.2 Juhiseid annab suunis G14 "Rakendussüsteemide läbivaatus".

1.1.3 Juhiseid annab suunis G17 "Auditivälise rolli mõju IS audiitori sõltumatusele".

1.1.4 Juhiseid annab suunis G20 "Aruandlus".

1.2 Seos COBITiga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- soorituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jäämise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusе indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

G23 Süsteemi arengu elutsükli (SAE) läbivaatused (jätkub)

1.3 Suunise vajadus

1.3.1 Organisatsioonid võtavad oma tegevusalaste tööde toeks kasutusele rakendussüsteeme. Rakendussüsteemide määratlemise, hankimise ja evitamise protsess sisaldab mitmesuguseid järke, nõuete tuvastusest rakendussüsteemi tegeliku evitamiseni ja üldiselt nimetatakse seda süsteemi arengu elutsükliks (SAE).

1.3.2 See suunis on mõeldud andma IS audiitoritele vajalikke juhiseid rakendussüsteemide SAE läbivaatuste sooritamiseks.

2 SÜSTEEMIDE ARENGU ELUTSÜKKEL

2.1 Määratlus

2.1.1 Süsteemi arengu elutsükkel on protsess, mis sisaldab mitu järku (alates teostatavuse väljaselgitamisest ja lõpetades teostusjärgsete läbivaatustega) ja millega juhtkonna mingi vajadus muundatakse rakendussüsteemiks, mis töötatakse välja individuaalsena, ostetakse või saadakse mõlema võimaluse kombinatsioonina.

2.2 Elutsüklit mõjutavad tegurid

2.2.1 Rakendussüsteemi SAE sõltub valitud hankimis- või väljatöötamisviisist. Rakendussüsteeme võidakse hankida või välja töötada mitmel viisil, sealhulgas

- individuaalväljatöötena, sisemisi ressursse kasutades;
- individuaalväljatöötena, täielikult või osaliselt väljasttellitavaid kohapealseid või mujal asuvaid ressursse kasutades;
- tarnijate tarkvarapakettidena, mis evitatakse kohandamiseta;
- tarnijate tarkvarapakettidena, mis kohandatakse konkreetsete vajaduste rahuldamiseks.

Mõnikord võivad suured keerukad rakendused kujutada endast kõigi ülalloetletud variantide kombinatsiooni.

2.2.2 Mõned organisatsioonid kasutavad spetsiifilisi SAE-metoodikaid ja protsesse, eriväljatöötena või tarnijalt saaduna. Üldiselt kirjutavad need ette tüüpprotsesse mitmesuguste soetamisviiside puhuks, võimaldades kohandada protsessi lahendust konkreetsete rakendussüsteemide tarbeks. Neid võivad toetada asjakohased SAE halduse instrumendid. Sellistel juhtudel sõltub SAE metoodikast või instrumendist.

2.2.3 Kui rakendussüsteemi ei osteta paketina, vaid töötatakse välja, sõltub SAE kasutatavast väljatöötuse metoodikast (näiteks koskarendus, prototüüpimine, kiirarendus, CASE, objektorienteeritud arendus).

G23 Süsteemi arengu elutsükli (SAE) läbivaatused (jätkub)

2.3 Elutsükli riskid

2.3.1 Rakendussüsteemi SAE kestel võivad ähvardada mitmesugused riskid, sealhulgas

- ebasobiva SAE kohaldamine rakendussüsteemile,
- puudulikud juhtimismeetmed SAE protsessis;
- rakendussüsteem ei vasta kasutaja nõuetele ja eesmärkidele;
- huvipoole (sealhulgas siseauditi) puudulik osalus;
- juhtkonnapoolse toetuse puudumine;
- puudulik projektijuhtimine;
- ebasobiv tehnoloogia ja arhitektuur;
- käsitlusala varieerumine;
- tähtaegade ületamine;
- ülekulud;
- rakendussüsteemi puudulik kvaliteet;
- ebapiisav tähelepanu rakendussüsteemi turvalisususele ja turvameetmetele (sealhulgas valideerimistele ja kontrolljälgedele);
- lahknevus sooritusvõime kriteeriumidest;
- ressursside või personaliga varustamise mudeli väär haldus;
- personali puudulikud oskused;
- ebapiisav dokumentatsioon;
- ebapiisav lepingukaitse;
- valitud SAE- ja/või väljatöötusmetoodikate puudulik järgimine;
- ebapiisav tähelepanu vastastikustele sõltuvustele muudest rakendustest ja protsessidest;
- puudulik konfiguratsioonihaldus;
- andmete konversiooni või migratsiooni ja ümberlülituse ebapiisav plaanimine;
- tegevuse katkemine pärast ümberlülitust.

3 PLAANIMINE

3.1 Tegurid, mida arvestada plaanimisel

3.1.1 Rakendussüsteemi SAE läbivaatuse plaanimisel peaks IS audiitor arvestama

- rakendussüsteemi hankimis- või väljatöötusviisi, tehnoloogiat, mahtu, eesmärke ja kavatsetavat kasutamist;
- hankimise ja evituse projekti struktuuri;
- projektirühma oskuste ja kogemuste profiili;
- valitud SAE mudelit;
- võimalikku rakendatavat SAE metoodikat ja kohandatud protsessilahendust;
- tõenäolisi SAE-d ähvardavaid riske;
- vastavale juhtkonnale ilmnenud võimalikke probleeme;
- SAE praegust järku;
- kõiki varasemaid rakendussüsteemi SAE eelmiste järkude läbivaatusi;
- kõiki varasemaid analoogilise rakendussüsteemi SAE läbivaatusi;
- kõiki pakutava läbivaatuse suhtes asjassepuutuvaid muid riski hindamisi või läbivaatusi, mida on sooritanud IS audiitor või teised (näiteks IT);
- kasutadaolevate IS audiitorite oskuste ja kogemuste taset ning pädeva välise abi saamise võimalust seal, kus see on vajalik.

3.2 Lähtetingimused

3.2.1 Ülaltoodut arvestades peaks IS audiitor jõudma plaanitava SAE läbivaatuse lähtetingimusteni. Selles dokumendis tuleks esitada

- läbivaatuse eesmärgid;
- läbivaatuse käsitlusala, väljendatuna läbivaatusega kaetavate SAE järkudena;
- läbivaatuse tüüp: pakutava SAE teostuseelne läbivaatus, paralleelne läbivaatus SAE järkude sooritamisel või teostusjärgne läbivaatus pärast kõnealuste SAE järkude lõpetamist;
- läbivaatuse kestus: tõenäolised alguse ja lõpu kuupäevad;
- leidudest ja soovitustest teatamise protsess;
- kokkulepitud meetmete järelkäsitluse protsess.

3.2.2 Valitud rakendussüsteemi SAE pakutava läbivaatuse kohta peaks IS audiitor leppima kokku vastava juhtkonnaga.

4 PÄDEVUS

4.1 Oskused ja kogemus

4.1.1 SAE läbivaatust sooritama määratud IS audiitoritel peaksid olema vajalikud oskused ja kogemused läbivaatuse kuluefektiivseks ja tõhusaks sooritamiseks. Kui on

kasutusel spetsiifilised SAE metoodikad ja vahendid, peaksid IS audiitoritel olema adekvaatsed teadmised ja kogemused niisuguste metoodikate ja vahendite ning nendega seotud riskide alal. Kui rakendussüsteemi ei osteta tarnijalt, vaid töötatakse välja, peaksid IS audiitoril analoogiliselt olema piisavad teadmised ja kogemused kasutatavate arendusmetoodikate ja -vahendite (näiteks koskarenduse, prototüüpimise, kiirarenduse, CASE, objektorienteeritud arenduse) alal. Kui see on õigustatud, peaks IS audiitor otsima sisemiste kasutadaolevate oskuste täiendamiseks väliseid ressursse (mis alluvad kohaldatavatele poliitikatele, protseduuridele ja kinnitustele).

5 SÕLTUMATUS

5.1 Sõltumatus

5.1.1 Rakendussüsteemi SAE läbivaatamisel peaks IS audiitor tegelikult ja nähtavalt olema sõltumatu projektirühmast, kelle kohustus on rakendussüsteemi hankimine ja evitamine. Selles kontekstis tuleks arvestada suunist G17, mis annab juhiseid selle kohta, kuidas auditiväline roll mõjutab IS audiitori sõltumatust.

6 LÄBIVAATUSETÖÖ SOORITAMINE

6.1 Läbivaatuste tüübid

6.1.1 IS audiitor peaks sooritama SAE läbivaatuse kooskõlas lähtetingimustega, mis on kokku lepitud vastava juhtkonnaga.

- Kui läbivaatus on teostuseelne läbivaatus, peaks IS audiitor uurima pakutavat SAE mudelit ja sellega seotud aspekte eesmärgiga hinnata nende sobivust ja võimalikke riske ning anda asjakohasele juhtkonnale vajalikke soovitusi riski leevendamiseks.
- Paralleelsete läbivaatuste puhul peaks IS audiitor vaatama läbi asjassepuutuvad SAE järgud nende asetleidmise ajal, eesmärgiga tuua esile riskid ja anda asjakohasele juhtkonnale vajalikke soovitusi riski leevendamiseks.
- Teostusjärgsete läbivaatuste puhul peaks IS audiitor asjassepuutuvad SAE järgud läbi vaatama pärast nende lõpuleviimist, eesmärgiga tõsta esile ilmnenud asjaolusid, et anda soovitusi paranduste tegemiseks järgmistes järkudes (kui see on võimalik) ja kasutada neid edaspidises õppevahendina.

6.2 Läbivaadatavad aspektid

6.2.1 Riskide ja probleemide ning nende toime hindamiseks peaks IS audiitor läbivaatuse käigus uurima ja hindama alljärgnevat. Mõned neist aspektidest puudutavad kõiki SAE läbivaatusi, sõltumata läbivaatuse tüübist (teostuseelne, paralleelne või teostusjärgne), mõned aga puudutavad ainult teatavaid läbivaatuse tüüpe. IS audiitor peaks uurima ja hindama neid aspekte, mis on pakutava läbivaatuse

G23 Süsteemi arengu elutsükli (SAE) läbivaatused (jätkub)

eesmärkide ja käsitlusala seisukohalt asjassepuutuvad, nii et ta jõuaks riskide ja probleemide asjakohase hindamiseni ning soovitusteni nende toime leevendamiseks; selliste aspektide hulka kuuluvad

- rakendussüsteemi projekti ülesanne (milles on projekti plaan, üleantavad saadused ja nende ajakavad) ja äriplaan (mis toob esile kulud ja tulud);
- projekti struktuur, sealhulgas kõik töörühmad ja juhtrühmad ning nendega seotud rollid ja kohustused;
- kasutatav formaalne projektihalduse metoodika (näiteks PRINCE 2), kui see on olemas, ja sellega seotud protsess, millega luuakse kohandatud protsessilahendusi;
- rakendussüsteemi jaoks valitud arenduse või rakenduse arenduse metoodika, näiteks koskarendus, prototüüpimine, kiirarendus, CASE, objektorienteeritud arendus, ja sellega seotud vahendid;
- tarnijatega sõlmitud lepingud hangitud rakendussüsteemide kohta;
- väljasttellitavate teenuste, näiteks kohandamise ja/või väljatöötuse tarnijatega sõlmitud lepingud;
- juhtimisprotsessid SAE mudelis, sealhulgas läbivaadatavatele SAE järkudele kohaldatavad läbivaatused, valideerimised, vastuvõtmised ja kinnitamised;
- läbivaadatavatest SAE järkudest üleantavate saaduste struktuur;
- asjassepuutuvate nõupidamiste (näiteks töörühma nõupidamise ja juhtrühma nõupidamise) protokollid
- tegelikud üleantavad saadused ning nende läbivaatuste ja kinnitamise kontrolljäljed;
- projekti aruandlus, edenemise jälgimine (panused, aeg, kulud) ja laiendamine;
- ressursihaldus;
- pidev riskihaldus;
- kvaliteedihaldus ja kvaliteedi tagamine;
- muudatuste haldus;
- soorituse ja probleemide haldus, sealhulgas teenusetasemelepped (SLA);
- konfiguratsioonihaldus;
- andmete konversioon ja migratsioon;
- projektisiseste läbivaatustega seotud dokumentatsioon, sealhulgas testimise kohta;
- projektisisene suhtlus ja suhtlus tarnijatega;
- rakendussüsteemi eelmiste SAE järkude läbivaatused (kui neid oli);

- analoogiliste rakenduste eelnenud SAE läbivaatused (kui neid oli);
- asjassepuutuvad õiguslikud, regulatiivsed ja poliitikate vastavusaspektid, kui neid on.

6.2.2 Rakendussüsteemide hankimise kohta määratleb COBIT laiad juhtimiseesmärgid, mis hõlmavad selliseid alasid nagu "Tuvastada automatiseeritud lahendused" (HE1) ja "Hankida rakendustarkvara ja hooldada seda" (HE2). Analoogilised laiad juhtimiseesmärgid käsitlevad projektide haldust (PO10), kvaliteedi haldust (PO8) ja süsteemi turvalisuse tagamist (TT5). COBITis on need eesmärgid liigendatud detailseteks juhtimiseesmärkideks. Läbivaatuse ühe osana peaks IS audiitor hindama nende juhtimiseesmärkide (mis puudutavad läbivaadatavaid SAE järke) saavutamise ulatust ning selliste eesmärkide saavutamiseks rakendatavate mehhanismide ja protseduuride toimivust.

6.2.3 COBIT määratleb ka seitse teabe kriteeriumi (toimivus, tõhusus, konfidentsiaalsus, terviklus, käideldavus, vastavus ja usaldatavus), millele peavad vastama rakendussüsteemid. Rakendussüsteemi SAE läbivaatuse ühe osana peaks IS audiitor hindama ka seda, kui toimivalt annavad läbivaadatavad SAE protsessid ja järgud oma panuse nende kriteeriumide rahuldamiseks. Rakendussüsteemi neile kriteeriumidele vastavuse tegelik hindamine on rakendussüsteemi läbivaatuse üks osa (vt suunis G14 "Rakendussüsteemide läbivaatus").

7 ARUANDLUS

7.1 IS audiitori aruanne

7.1.1 Rakendussüsteemide SAE läbivaatuste puhul võidakse aruanded sageli koostada järk-järgult, sedamööda, kuidas tuvastatakse riskid ja probleemid. Niisugused aruanded tuleks vajalike meetmete rakendamiseks adresseerida asjakohasele juhtkonnale. Väljastada võidakse lõpparuanne, mis loetleb kõik läbivaatuse ajal kerkinud probleemid.

7.1.2 Aruandes tuleks sõltuvalt läbivaatuse tüübist käsitleda selliseid aspekte nagu

- SAE mudeli ja arendusmetoodika sobivus;
- riskid ja probleemid, nende põhjused ja toime;
- võimalikud riski leevendamise meetmed SAE läbivaatusel olevas järgus või sellele järgnevates järkudes. Näiteks võivad mõned kavandamisjärgus ilmnenud asjaolud nõuda meetmeid riski leevendamiseks järgmistes järkudes, näiteks väljatöötamise ja testimise ajal.

G23 Süsteemi arengu elutsükli (SAE) läbivaatused (jätkub)

8 JÄRELTOIMINGUD

8.1 Õigeaegsed järeltoimingud

8.1.1 Rakendussüsteemide SAE läbivaatuste, eriti teostuseelsete ja paralleelsete läbivaatuste puhul tuleks sooritada asjakohased järeltoimingud mõistliku kinnituse saamiseks sellele, et riski leevendamise meetmed rakendatakse õigeaegselt. Teostusjärgsete läbivaatuste puhul peaksid järeltoimingud keskenduma parandusmeetmete õigeaegsusele järgmistes järkudes ja analoogilistes tulevastes projektides.

9 JÕUSTUMISKUUPÄEV

9.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. augustil 2003 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

LISA

Toetumine COBITile

Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ja arvestades COBITi teabekriteeriume.

Käesoleva konkreetse auditiala, SAE läbivaatuse puhul on COBITi protsessidest tõenäoliselt kõige asjakohasemad mõned plaanimise ja organiseerimise IT-protsessid, kõik hankimise ja evituse IT-protsessid ning mõned tarne ja toe protsessid. Niisiis tuleks auditi sooritamisel lugeda asjassepuutuvaiks COBITi juhiseid järgmiste protsesside kohta:

- PO8 – Tagada vastavus välisnõuetele (COBIT v3)
- PO10 – Hallata projekte
- PO11 – Hallata kvaliteeti (COBIT v3)
- HE1 – Tuvastada automatiseeritud lahendused
- HE2 – Hankida rakendustarkvara ja hooldada seda
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE4 – Võimaldada käitus ja kasutamine
- HE5 – Hankida IT-ressursid
- HE6 – Hallata muutusi

G23 Süsteemi arengu elutsükli (SAE) läbivaatused (jätkub)

- TT1 – Määratleda teenusetasemed ja hallata neid
- TT2 – Hallata kolmandate osapoolte teenuseid
- TT3 – Hallata suutlikkust ja võimsust
- TT4 – Tagada pidev teenus
- TT5 – Tagada süsteemide turvalisus
- TT7 – Koolitada kasutajaid

SAE auditi puhul on kõige asjakohasemad teabekriteeriumid

- esmajärjekorras: toimivus ja tõhusus;
- seejärel: konfidentsiaalsus, terviklus, käideldavus, vastavus, usaldatavus.

G24 Interneti-pangandus

1 TAUST

1.1 Seos ISACA standarditega

1.1.1 Standard S2 "Sõltumatus" määrab: "IS auditi talitus peaks auditiülesande objektiivseks sooritamiseks olema sõltumatu läbivaadatavast tegevusvaldkonnast."

1.1.2 Standard S4 "Kutsealane pädevus" määrab: "IS audiitor peaks olema kutsealaselt pädev, tal peaksid olema auditiülesande täitmiseks vajalikud oskused ja teadmised."

1.1.3 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.4 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite sobiva analüüsi ja tõlgendamisega."

1.1.5 Juhiseid annab suunis G22 "Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus".

1.1.6 Juhiseid annab protseduur P3 "Sissetungi tuvastuse süsteemi (IDS) läbivaatus".

1.1.7 Juhiseid annab protseduur P2 "Digitaalallkirjad ja võtmehaldus".

1.2 Seos COBITiga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- soorituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jäämise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusse indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

1.3 Suunise vajadus

1.3.1 Selle suunise eesmärk on kirjeldada soovitatavaid tavasid Interneti-panganduse ürituste, rakenduste ja teostuste läbivaatuse sooritamiseks ning aidata tuvastada ja ohjata riske, mis on seotud selle tegevusega, nii et läbivaatuse käigus järgitaks asjassepuutuvaid IS auditeerimise standardeid.

2 INTERNETI-PANGANDUS

2.1 Määratlus

2.1.1 Termin "Interneti-pangandus" tähendab Interneti kasutamist kaugedastuse kanalina pangandusteenuste tarbeks. Teenuste hulka kuuluvad traditsioonilised, näiteks konto avamine või summade ülekandmine mitmesugustele kontodele, ning uued pangandusteenused, näiteks elektroonilised interaktiivsed maksed (mis võimaldavad klientidel saada ja maksta panga veebisaidis arveid).

2.2 Interneti-panganduse toimingud

2.2.1 Üha suurem arv panku korraldab oma äritegevust ümber, kasutades Interneti-tehnoloogiat oma kliendisuhete arendamiseks või laiendamiseks. Millises ulatuses kasutatakse pangas Internetti, sõltub panga suhtelisest küpsusest Interneti-tehnoloogia osas. Pangad pakuvad Interneti-pangandust põhiliselt kahel viisil. Olemasolev füüsiliste kontoritega pank, mida harilikult nimetatakse kivist pangaks, võib rajada veebisaidi ja pakkuda oma klientidele Interneti-pangandust ühe täiendusena lisaks oma traditsioonilistele tarnekanalitele. Alternatiiv on asutada virtuaalne, harukontoriteta ehk puht-Interneti-pank. Virtuaalpanga keskmes asuv serverarvuti või panga andmebaas võib paikneda sellise panga juriidiliseks aadressiks olevas kontoris või mingis teises asukohas. Virtuaalpangad võimaldavad kasutajail raha hoiule panna ja välja võtta rahaautomaatide (ATM) kaudu või muude, teistele asutustele kuuluvate kaugedastuskanalite kaudu. Interneti-panganduse erijooned on enneolematu muutumiskiirus, mis on seotud tehnoloogia ja klienditeeninduse uuendusega, Interneti kõikjalolev ja ülemaailmne iseloom, Interneti-panganduse rakenduste integratsioon

pärand-arvutisüsteemidega ning pankade üha suurem sõltuvus kolmandatest pooltest, kes annavad vajaliku infotehnoloogia. Vastavalt ülalöeldule saab pank sooritada oma Interneti-tegevusi ühel või mitmel viisil alljärgnevate hulgast.

- Teabelised. See on Interneti-panganduse algtase. Tüüpiliselt asub panga turundusteave panga toodete ja teenuste kohta mingil autonoomsel serveril. Selliste operatsioonidega seotud riskid on suhteliselt väikesed, sest tavaliselt ei ole infosüsteemidel mingit teed serveri ja panga sisemise võrgu vahel. Sellel tasemel Interneti-pangandust võib pakkuda pank ise või ta võib selle tellida väljastpoolt. Panga risk on küll suhteliselt väike, kuid serveril või veebisaidis olevad andmed võivad olla avatud muutmise ohule. Seetõttu tuleb panga serveril või veebisaidis olevate andmete lubamatu muutmise vältimiseks rakendada sobivaid meetmeid.
- Suhtluslikud. Sellist tüüpi Interneti-panganduse süsteem võimaldab mõningat interaktsiooni panga süsteemide ja kliendi vahel. See interaktsioon võib piirduda meiliga, kontopäringuga, laenutaotlustega või staatiliste failide ajakohastusega (nimede ja aadresside muutmisega). Kuna sellistel serveritel on tavaliselt otsetee panga sisemistesse võrkudesse, on selle konfiguratsiooni puhul operatsioonide risk suurem kui teabelistes süsteemides. Kasutusel peaksid olema meetmed, millega vältida, seirata ja alarmeerida juhtkonda kõigist volitamata katsetest pääseda panga sisemistesse võrkudesse ja arvutisüsteemidesse. Selle keskkonnas on tähtsad ka viiruste avastamise ja vältimise meetmed.
- Tehingulised. See Interneti-panganduse tase võimaldab klientidel otseselt sooritada rahaliste tagajärgedega tehinguid. Tehingulisel Interneti-pangandusel on kaks taset; nende riskiprofiilid on erinevad. Elementaarne tehingusait võimaldab ainult rahasummade ülekandmist ühe kliendi kontode ja panga vahel. Arenenum tehingusait annab vahendid maksete genereerimiseks otse kolmandatele väljaspool panka. Seda saab teha arvemaksete kujul, pangatšeki kaudu või elektroonilise arvelduse kirjetega. Paljud pangad pakuvad ka makseid kliendilt kliendile, kasutades üht neist maksemeetoditest. Kui summasid võimaldatakse üle kanda mingisse kohta väljaspool panka, suureneb tegevusrisk. Volitamata juurdepääs võib selles keskkonnas viia pettuseni või kutsuda seda esile. Kuna ühendusteed on tavaliselt keerukad ning võivad kulgeda kliendi ja panga sisemiste võrkude vahel läbi mitme avaliku serveri, liini või seadme, on sellisele arhitektuurile omane suur risk ja sellele tuleb rakendada kõige tugevamaid turvameetmeid.

3 INTERNETI-PANGANDUSE LÄBIVAATUS

3.1 Käsitlusala

3.1.1 Pangandus on juba oma loomult suure riskiga äritegevus. Suuremad pangandustegevustega seotud riskid on strateegilised, maineriskid, tegevusriskid (nende hulka kuuluvad turvariskid – mõnikord nimetatakse neid tehinguriskideks – ja õiguslikud riskid), krediidi-, hinna-, valuuta-, intressimäära- ja likviidsusriskid.

G24 Interneti-pangandus (jätkub)

Interneti-panganduse tegevused ei tekita riske, mida ei tuntud juba traditsioonilises panganduses, kuid nad suurendavad ja muudavad mõningaid neist traditsioonilistest riskidest. Põhitegevus ja IT-keskkond on omavahel tihedalt seotud, see aga mõjutab Interneti-panganduse üldist riskiprofiili. Konkreetsemalt, IS audiitori seisukohalt on peamised probleemid strateegiline, tegevus- ja mainerisk, sest need on otseselt seotud ohtudega usaldatavale andmevoole ning neid suurendab Interneti-panganduse kiire kasutuselevõtt ja selles peituv tehnoloogiline keerukus. Pankadel peaks olema riskihalduse protsess, mis võimaldaks neil tuvastada, mõõta, seirata ja ohjata enda avatust tehnoloogiariskidele. Uute tehnoloogiate riskihaldusel on kolm olulist elementi.

- Riskihaldus on juhatuse ja kõrgema juhtkonna kohus. Nad vastutavad panga äristrateegia väljatöötamise eest ja toimiva riskihalduse metoodika kehtestamise eest. Neil peavad olema teadmised ja oskused panga Interneti-kasutuse ja kõigi sellega seotud riskide haldamiseks. Juhatus peaks tegema selgesõnalise, põhjendatud ja dokumenteeritud otsuse selle kohta, kas ja kuidas peab pank andma Interneti-panganduse teenuseid. Algne otsus peaks hõlmama kõiki spetsiifilisi vastutusi, poliitikaid ja meetmeid riskide, sealhulgas piiriületuse kontekstis tekkivate riskide käsitluseks. Juhatus peaks läbi vaatama, kinnitama ja allutama seirele Interneti-panganduse tehnoloogiaga seotud projektid, mis oluliselt mõjutavad panga riskiprofiili, ning kindlustama adekvaatsete meetmete väljaselgitamise, plaanimise ja rakendamise.
- Tehnoloogia rakendamine on infotehnoloogia kõrgema juhtkonna kohus. Tal peaksid olema oskused Interneti-panganduse tehnoloogiate ja toodete toimivaks hindamiseks ning nende sobiva installeerimise ja dokumenteerimise kindlustamiseks. Kui pangal ei ole asjatundmist selle kohustuse täitmiseks oma jõududega, peaks ta kaaluma lepingu sõlmimist tarnijaga, kes on spetsialiseerunud sellel tegevusalal, või võtma liitlaseks muu kolmanda poole, kes saab teda täiendada tehnoloogia või asjatundmisega.
- Riski mõõtmine ja seire on tegevjuhtkonna kohus. Tal peaksid olema oskused Interneti-pangandusega seotud riskide toimivaks tuvastuseks, mõõtmiseks, seireks ja ohjeks. Juhatus peaks saama regulaarseid aruandeid rakendatavate tehnoloogiate, eeldatavate riskide ja nende riskide halduse kohta.

3.1.2 Interneti-pangandusele rakendatavad sisemised meetmed peaksid olema proportsioonis panga pakutavate teenuste riski suurusega, teostuses sisalduva riski suurusega ja panga riskitaluvuse suurusega. Sisejuhtimise läbivaatus Interneti-panganduse keskkonnas peab aitama IS audiitoril saada mõistlikku kinnitust sellele, et meetmed on sobivad ja töötavad asjakohaselt. Üksikpanga Interneti-panganduse tehnoloogia ja toodete juhtimiseesmärgid võiksid keskenduda alljärgnevale.

- Tehnoloogia plaanimise ja strateegiliste sihtide kooskõla, sealhulgas tegevuse toimivus, tõhusus ja ökonoomsus ning vastavus üleorganisatsioonilistele poliitikatele ja õigusnormidele.
- Andmete ja teenuste käideldavus, sealhulgas äritegevuse taaste plaanimine.
- Andmete terviklus, sealhulgas varade kaitsmine turvameetmetega, tehingute korralik volitamine ja andmevoo usaldatavus.

G24 Interneti-pangandus (jätkub)

- Andmete konfidentsiaalsuse ja privaatsuse standardid, sealhulgas meetmed nii töötajate kui ka klientide juurdepääsu reguleerimiseks.
- Juhtkonnale adresseeritud aruandluse usaldatavus.

3.1.3 Sisemiste meetmete ja nende adekvaatsuse asjakohaseks hindamiseks peaks IS audiitor tundma panga tegevuskeskkonda. COBITi 3. redaktsioon, mille IT Halduse Instituut avaldas aastal 2000, esitab seitse teabekriteeriumi, mida infosüsteemid peavad rahuldama:

- toimivus,
- tõhusus,
- konfidentsiaalsus,
- terviklus,
- käideldavus,
- vastavus,
- usaldatavus.

3.1.4 Selle dokumendi jaotises 3.1.3 loetletud teabekriteeriumid on Interneti-panganduse puhul asjassepuutuvad. Seetõttu peaks Interneti-panganduse läbivaatus käsitlema seda, kuidas Interneti-panganduse üritus, rakendus või teostus rahuldab COBITi teabekriteeriume.

3.1.5 Pangandustegevuste muude vormide või kanalitega võrreldes sõltub Interneti-panganduse tugevalt kliendi andmete terviklusest ja usaldatavast konfidentsiaalsusest ning süsteemi käideldavusest. Selles kontekstis peaksid olema kasutusel sobivad liiasuse ja taanderežiimi laskumise võimalused ning avariijärgse taaste protseduurid. Makseid ja rahaülekandeid sisaldava Interneti-panganduse puhul on olulised atribuudid salgamise vääramine ja tehingute terviklus. Sellistel juhtudel peaks Interneti-panganduse läbivaatus käsitlema Interneti-panganduse süsteemi turvameetmete toimivust salgamise vääramise ja andmetervikluse tagamisel. Sellele tuleks pöörata vajalikku tähelepanu Interneti-panganduse lahenduste käideldavuse hindamisel, eriti siis, kui pidevus põhineb piire ületaval töötlusel, sest see võib rikkuda õigusnorme või olla vastuolus panga eeskirjadega.

3.1.6 Interneti-panganduses on oluline tõendada, et iga suhtlus, tehing ja pääsutaotlus on seaduslik. Seetõttu peaksid pangad kasutama usaldusväärseid meetodeid uute klientide identiteedi verifitseerimiseks ja nende volitamiseks, samuti elektroonilisi tehinguid algatada püüdvate juba vormistatud klientide identiteedi ja volituste kontrollimiseks. Varguse, pettustehingute ja rahapesutoimingute riski vähendamiseks on tähtis kliendi verifitseerimine konto avamisel. Klientide tugeva identifitseerimise ja autentimise protsessid on eriti tähtsad piiriületuse kontekstis, sest klientidega elektroonilise äri tegemisel üle riigisiseste või riikidevaheliste piiride võib tekkida raskusi, sealhulgas identiteedi teesklemise risk ja raskused võimalike klientide toimiva krediidikontrolli läbiviimisel.

G24 Interneti-pangandus (jätkub)

3.1.7 Auditeeritavusel on Interneti-panganduse keskkonnas suurem tähtsus, sest oluline osa tehingutest toimub paberita keskkondades.

4 SÕLTUMATUS

4.1 Kutsealane objektiivsus

4.1.1 Enne ülesande vastuvõtmist peaks IS audiitor andma mõistliku kinnituse sellele, et mitte mingid tema võimalikud huvid läbivaadatavas Interneti-pangas ei kahjusta mitte mingil viisil läbivaatuse objektiivsust. Igasuguse võimaliku huvide vastuolu puhul tuleks sellest selgesõnaliselt teatada panga juhtkonnale ning enne ülesande vastuvõtmist tuleks panga juhtkonnalt saada kirjalik nõusolek.

5 PÄDEVUS

5.1 Oskused ja teadmised

5.1.1 IS audiitoril peaksid olema Interneti-panganduses rakendatava tehnoloogia ja Interneti-pangandusega seotud riskide läbivaatuseks vajalikud tehnilised ja tegevusalased oskused ja teadmised. IS audiitor peaks välja selgitama, kas tehnoloogia ja tooted on kooskõlas panga strateegiliste sihtidega. Eriti nõuavad sellised läbivaatused pangaoperatsioonide ja nendega seotud riskide tundmist, pangandust puudutavate õigusaktide tundmist ning tehnilisi teadmisi, mis on vajalikud selliste aspektide hindamiseks nagu veebimajutuse tehnoloogiad, krüpteerimistehnoloogiad, võrguturbe arhitektuur ja turbe tehnoloogiad, näiteks tulemüürid, sissetungi tuvastus ja viirusetõrje. Kui on vaja saada nõuandeid või teavet välistelt asjatundjatelt, tuleks asjakohaselt kasutada väliseid erialaressursse. Väliste asjatundmisressursside võimaliku kasutamise fakt tuleks panga juhtkonnale kirjalikult teatavaks teha.

6 PLAANIMINE

6.1 Üldine riski kaalutlemine

6.1.1 IS audiitor peaks koguma teavet panga Interneti-panganduse eesmärkide kohta, nende eesmärkide saavutamiseks kasutatava strateegia kohta ja selle kohta, mil viisil kasutab pank Interneti-tehnoloogiat oma suhetes klientidega (teabeliselt, suhtluslikult või tehinguliselt, vt 2.2.1). SEl viisil kogutav teave peaks olema niisugune, mis aitab viia läbi pangandusriskide ja COBITi teabekriteeriume puudutavate riskide üldise kaalutlemise. Selline üldine riski kaalutlemine aitab määrata läbivaatuse käsitlusala ja katvust. Kui pangal on mingi ettevõtteriski raamstruktuur, võib kasutada seda.

G24 Interneti-pangandus (jätkub)

6.1.2 IS audiitor peaks järgima mingit riski kaalutlemise metoodikat, millega analüüsida ja hinnata Interneti-panganduse rakendamisega seotud peamisi võimalikke üldisi ja spetsiifilisi ohte, nende võimalikke realiseerumisi, võimalikku toimet pangale, realiseerumiste tõenäosusi ning võimalikke riskihalduse meetmeid, mida saab rakendada riskide vältimiseks. Hinnata tuleks järgmised strateegiariskid:

- strateegiline hindamine ja riskianalüüs;
- integratsioon üleorganisatsiooniliste strateegiliste sihtidega;
- tehnoloogilise infrastruktuuri valimine ja haldus;
- kolmandatelt pooltelt tellimise suhete halduse igakülgne protsess.

6.1.3 Hinnata tuleks järgmised turvariskid:

- klientide turbetavad;
- klientide autentimine;
- tehingute jälitatavus ja salgamise vääramine;
- kohustuste lahusus;
- volituste kontrolli mehhanismid süsteemides, andmebaasides ja rakendustes;
- sisemine või väline pettus;
- tehingute, andmebaaside ja kirjete andmeterviklus;
- tehingute kontrolljäljed;
- andmete konfidentsiaalsus edastuse ajal;
- kolmandate pooltega seotud turvarisk.

6.1.4 Hinnata tuleks järgmised õigusriskid:

- teabe paljastamised klientidele;
- privaatsus;
- vastavus seadustele, eeskirjadele ja reguleerija või järelevalvaja nõuetele;
- allumine võõrjurisdiktsioonidele.

6.1.5 Hinnata tuleks järgmised maineriskid:

- teenusetaseme andmine;
- kliendi eest hoolitsemise tase;
- jätkusuutlikkuse ja ootamatuste käsitluse plaanimine.

G24 Interneti-pangandus (jätkub)

6.2 Läbivaatuse käsitlusala ja eesmärgid

6.2.1 IS audiitor peaks, vajadusel panga juhtkonnaga konsulteerides, selgelt määratlema Interneti-panganduse läbivaatuse käsitlusala ja eesmärgid. Läbivaatusega kaetavad aspektid tuleks selgelt sõnastada käsitlusala ühe osana. Panga Interneti-tegevuste iseloom ja Interneti-panganduse tegevuste maht (mis on kirjeldatud jaotises 2.2.1) ning nendega seotud riskid (mis tuvastati üldise riskikaalutlusega) dikteerivad selle, millised aspektid tuleb läbi vaadata, samuti läbivaatuse ulatuse ja sügavuse.

6.2.2 Läbivaatuse otstarbeks peaksid juhtimiseesmärgid vastama eeskirjadele ja kohaldatavatele pangandusseadustele. Internetil pole piire, seetõttu saab iga pank raskusteta kasutada Interneti-põhist ühenduskanalit tegutsemiseks mitme osariigi ja ka mitme riigi keskkonnas. Pank võib avastada, et teda seovad mitte ainult tema füüsilise asukoha õigusnormid ja tavad, vaid ka ta klientide kõigi asukohtade omad. Seetõttu peaks IS audiitor tegema kindlaks panga praeguse ja ka plaanilise klientuuri geograafilise paiknemisala. IS audiitoril on vaja välja selgitada, mitme eri jurisdiktsiooni õigusliku ja regulatiivse kontrolli all on Interneti-panganduse töö, ja teha kindlaks, kuidas Interneti-pank haldab sellest tulenevat riski.

6.3 Metoodika

6.3.1 IS audiitor peaks sõnastama metoodika nii, et läbivaatuse käsitlusala ja eesmärgid saaks saavutada objektiivsel ja professionaalsel viisil. Järgitav metoodika peaks sõltuma sellest, kas läbivaatus on teostuseelne või teostusjärgne läbivaatus. Metoodika tuleks sobivalt dokumenteerida. Kui tuleb kasutada väliste asjatundjate teavet või nõuandeid, tuleks ka see asjaolu spetsifitseerida metoodika ühe osana.

6.4 Plaani kinnitamine

6.4.1 Sõltuvalt organisatsiooni tavadest on IS audiitoril võib-olla sobiv saada läbivaatuse plaani ja metoodika kohta saada panga juhtkonna nõusolek.

7 INTERNETI-PANGANDUSE LÄBIVAATUSE SOORITAMINE

7.1 Sooritamine

7.1.1 Läbivaadatavad aspektid ja läbivaatuse protsess tuleks valida arvestades läbivaatuse jaoks kavandatud käsitlusala ja eesmärki, samuti plaanimisprotsessi ühe osana määratletud metoodikat.

7.1.2 Üldiselt tuleks Interneti-panganduse kohta teabe kogumisel, analüüsimisel ja tõlgendamisel uurida olemasolevat dokumentatsiooni (näiteks panga eeskirju Interneti-panganduse kohta), Internetti puudutavaid seadusi, privaatsusseadusi, veebipanganduse süsteemi dokumentatsiooni ja Interneti-panganduse lahenduse kasutamist.

G24 Interneti-pangandus (jätkub)

7.1.3 Interneti-panganduse valdkonnaga seotud ning varem märkamata jäänud ja võib-olla järeltoiminguid nõudvate probleemide tuvastamiseks peaks IS audiitor vaatama läbi järgmised dokumendid:

- eelmiste uurimiste aruanded;
- järeltoimingud;
- eelmiste uurimiste töödokumendid;
- sise- ja välisauditite aruanded.

7.1.4 IS audiitor peaks kaardistama kesksed Interneti-panganduse ürituse või süsteemiga seotud protsessid, nii automatiseeritud kui ka käsitsi sooritatavad.

7.1.5 Kesksete äririskide (vt 6.1) kaalutlemine peaks sisaldama Interneti-panganduse eesmärkide, strateegia ja ärimudeli hindamist.

7.1.6 Seejärel peaks IS audiitor hindama nende protsessidega seotud tuvastatud riskide (nii äri- kui ka IS riskide) korraga materialiseerumise tõenäosust ja nende tõenäolist toimet ning dokumenteerima need riskid koos nende leevendamise meetmetega.

7.1.7 IS riski kaalutlemise ühe osana tuleks hinnata välised IS ohud, sõltuvalt panga pakutavate toodete iseloomust ja välistest ohtudest, mida tuleb arvestada. Nende ohtude hulka kuuluvad teenusetõkestus, volitamata juurdepääs andmetele, ja arvutiseadmete volitamata kasutamine, ning neid võivad algatada mitmesugused allikad: juhuslikud häkkerid, konkurendid, välisriikide valitsused, terroristid või rahulolematud oma töötajad.

7.1.8 Sõltuvalt teostuseelse või -järgse läbivaatuse iseloomust peaks IS audiitor testima olulisi protsesse test- ja töökeskkonnas, kontrollides, kas protsessid toimivad nii, nagu on kavatsetud. Nende testide hulka kuuluvad bilansipäringu testimine, arve esituse ja maksmise testimine ning turvamehhanismide testimine läbistustestimisega.

7.1.9 Teostusjärgsel läbivaatusel peaks IS audiitor saama ettekujutuse vähemalt võrgu topoloogiast, võrgu marsruutimisest, süsteemide ja võrgu turvalisuse hindamisest ning sisemisest ja välisest sissetungist.

7.1.10 Kuna Interneti-panganduse lahendus on valdavalt infotehnoloogiline lahendus, peaks ta vastama COBITis kehtestatud teabekriteeriumidele ning muudele asjassepuutuvatele selle valdkonna standarditele või eeskirjadele. Analüüsida tuleks neile teabekriteeriumidele, standarditele ja eeskirjadele vastavuse ulatust ja lahknevuste toimet.

7.2 Läbivaadatavad aspektid

7.2.1 Järgmiste organisatsiooniaspektide puhul tuleks läbi vaadata, kas

- enne Interneti-panganduse tegevuste läbiviimist on sooritatud hoolsus- ja riskianalüüs;
- piire ületavate tegevuste puhul on sooritatud hoolsus- ja riskianalüüs;

G24 Interneti-pangandus (jätkub)

- Interneti-pangandus on kooskõlas panga üldise missiooni, strateegiliste sihtide ja tööplaanidega;
- Interneti-rakendus vastab määratletud ja kinnitatud ärimudelile;
- Interneti-panganduse süsteeme ja/või teenuseid hallatakse oma jõududega või tellitakse haldus kolmandalt poolelt;
- organisatsiooni juhtkond ja personal ilmutavad Interneti-panganduse halduseks piisavaid teadmisi ja tehnilisi oskusi;
- on kasutusel meetmed kohustuste lahususe tagamiseks;
- aruanded juhtkonnale on adekvaatsed Interneti-panganduse tehingu- ja makseteenuste tegevuste asjakohaseks halduseks.

7.2.2 Läbivaatus peaks hõlmama näiteks järgmisi poliitikaaspekte, küsides, kas

- on määratletud ja kasutusel sobivad poliitikad, mis puudutavad klientide soetamist, sidemeid tarnijatega, klientide autentimist, klientide ja tarnijate andmete privaatsust, kontrolljälgi, kasutamislogide läbivaatust ja seda, kas pank hoiab end kooskõlas Interneti-pangandust puudutavate õigusalaste arengutega;
- pank tagab õiged privaatsuse paljastused, mis on seotud ta Interneti-panganduse tootesarjaga;
- veebisaidis antakse teave, mis võimaldab klientidel enne Interneti-panganduse teenuste kasutamist teha põhjendatud otsuseid panga identiteedi ja õigusliku seisundi kohta (panga nimi ja ta peakontori asukoht, panga esmane järelevalveorgan, klienditeenindusega ühenduse võtmise viisid ja muu asjassepuutuv teave);
- pank on kehtestanud poliitikad, mis suunavad hüperteksti linkide kasutamist, nii et tarbijad saaksid selgelt eristada panga tooteid muudest toodetest ning et neid panga veebisaidist lahkumisel teavitataks väljumisest;
- on kasutusel sobivad protseduurid muudatuste ohje, kontrolljälgede läbivaatuse ning kasutuslogide (tulemüürilogide ja muude teadete) läbivaatuse või analüüsimise tarbeks;
- on kasutusel sobivad ja adekvaatsed protseduurid, millega tagada andmete privaatsust ja terviklust ning kindlustada vastavust kehtivatele õigusnormidele ja parimatele tavadele.

7.2.3 Järgmiste plaanimisaspektide puhul tuleks läbi vaadata, kas

- plaanitud infosüsteemide tehnoloogia arhitektuur on teostatav ning annab tulemuseks ohutu ja turvalise talitluse;
- on olemas sobivad intsidentidele reageerimise plaanid, millega hallata, eraldada ja minimeerida probleeme, mida tekitavad ootamatud sündmused, sealhulgas sisemised või välised ründed;

G24 Interneti-pangandus (jätkub)

- on olemas "Interneti-toote elutsükkel" ning seda järgitakse Interneti-rakenduste väljatöötamisel, hooldamisel ja ajakohastamisel;
- on olemas elutähtsate Interneti-panganduse töötlus- ja/või edastussüsteemide jätkusuutlikkuse ja ootamatuste käsitluse plaanid ja neid testitakse regulaarselt.

7.2.4 Infosüsteemide infrastruktuuri järgmiste aspektide puhul tuleks läbi vaadata, kas

- pakutava äriplaaniga sobitamiseks saab infrastruktuuri ja süsteeme laiendada;
- infoturbe arhitektuur on määratletud ja sobib kavatsetud Interneti-panganduse mudeli iseloomuga;
- pangal on adekvaatne protsess ja meetmed Interneti-panganduse süsteemiga seotud riistvara, tarkvara ja andmesideseadmete füüsiliseks turbeks;
- pangal on usaldatav protsess, mis tagab, et tee veebisaidi ja panga sisemiste võrkude või arvutisüsteemide vahel on adekvaatselt kontrolli all, ning sisemine võrk on väliskeskkonna eest sobivalt kaitstud sobiva tulemüüritehnoloogia abil;
- andmebaasid ja andmevoog on kaitstud volitamata või väära juurdepääsu eest;
- kasutusel on sobivad ja adekvaatsed protseduurid, millega tagada pääsupunktide ja võimalike nõrkusealade identifitseerimine;
- on olemas sobivad käsitsi bilanseerimise meetmed juhtudeks, kus automaatsed vahendid on puudulikud;
- iga klienditehingu kirjes on kliendi identifikaator, tehingu number, tehingu tüüp, tehingusumma ja muu asjassepuutuv teave (kui seda salvestatakse ja arhiveeritakse) juhtimisotstarbeks või muudeks äriotstarveteks, näiteks turunduseks.

7.2.5 Andmeside infrastruktuuri järgmiste aspektide puhul tuleks läbi vaadata, kas

- võrgu arhitektuur sobib oma iseloomu, ajastuse ja ulatuse poolest Interneti-panganduse tööks;
- kasutatavad võrguprotokollid sobivad kavatsetud kasutamiseks (näiteks, kui maksed või ülekanded Interneti-panganduse süsteemi kaudu on lubatavad, tuleks kasutada turvalisi protokolle);
- pangal on mingi toimiv protsess, millega hinnata nende kasutuselolevate füüsiliste meetmete adekvaatsust, millega kitsendatakse juurdepääsu tulemüüri serveritele ja komponentidele;
- kasutusel on sissetungi tuvastuse süsteemid ja viirusetõrje süsteemid või protseduurid;
- kasutusel on adekvaatne sisemiste või väliste võrkude läbistustestimine;

G24 Interneti-pangandus (jätkub)

- vajalikel ja sobivatel juhtudel on suhtlus võrgu kaudu turvatud virtuaalse privaatvõrguga (VPN) ja sellega seotud krüpteerimismeetoditega;
- andmete kaitseks võrgusuhtluse ajal on valitud adekvaatsed ja tugevad krüpteerimisalgoritmid.

7.2.6 Järgmiste autentimisaspektide puhul tuleks läbi vaadata, kas

- kasutusel on turvafunktsioonid tulevaste klientide identiteedi valideerimiseks, kui nad kasutavad Internetti uute pangalaenu- või hoiusekontode taotlemiseks;
- süsteemidesse on ehitatud turvafunktsioonid, millega tagada olemasolevate klientide autentimist, andmeterviklust ja tehingute konfidentsiaalsust;
- vajaduse korral kasutatakse tehingupoole üheseks ja kindlaks identifitseerimiseks autentimisprotseduure, mis rakendavad digitaalsertifikaate ja -allkirju;
- tehingute tegemisel Interneti-panganduse süsteemi kaudu on tagatud salgamise vääramine võimalikuks tulevaseks äri- või õigusalaseks kasutamiseks;
- Interneti-panganduse süsteemi veataluvuse vahendid on õiges proportsioonis süsteemi iseloomu, mahu ja elutähtsusega.

7.2.7 Kolmandatest pooltest teenuseandjate järgmiste aspektide puhul tuleks läbi vaadata, kas

- enne ükskõik milliste lepingute sõlmimist kolmandast poolest teenuseandjaga on läbi viidud hoolikas pädevuse ja rahalise eluvõime läbivaatus;
- lepingud kolmandatest pooltest teenuseandjatega kaitsevad adekvaatselt panga ja ta klientide huve ning panga organisatsioon on läbi vaadanud tarnelepingud, veendudes, et iga osapoole kohustused on asjakohaselt piiritletud ja määratletud;
- panga organisatsioon saab kolmandatest pooltest teenuseandjate sise- või välisauditite aruandeid ja vaatab need läbi, hinnates tarnija halduse protsesse või spetsiifilisi tarnijasuhteid, mis on seotud infosüsteemide ja -tehnoloogiaga, ning kõik väljasttellitavad süsteemid ja tegevused alluvad riskihaldus-, turva- ja privaatsuspoliitikatele, mis vastavad panga enda standarditele;
- panga organisatsioonil on õigus viia läbi kolmandatest pooltest teenuseandjate turvalisuse, sisejuhtimise ning jätkusuutlikkuse ja ootamatusekäsitluse plaanide sõltumatuid läbivaatusi ja/või auditeid;
- juhul, kui Interneti-panganduse lahendus sõltub ükskõik millistest kolmandatest pooltest teenuseandjatest, näiteks Interneti-teenuseandjaist (ISP), serifitseerimiskeskusest (CA), registreerimiskeskusest (RA) või veebimajutuse agentuurist, on kolmandate poolte turbeprotseduurid sobivad ja adekvaatsed;
- kolmandatest pooltest teenuseandjatel on elutähtsate Interneti-panganduse töötlus- ja edastussüsteemide jaoks sobivad jätkusuutlikkuse ja ootamatusekäsitluse plaanid ja neid testitakse regulaarselt ning pank saab testimisaruannete eksemplare;

- pangal, kui ta saab tarnijalt tarkvaratooteid, on adekvaatne protsess, millega tagada, et tarnija hooldatav tarkvara on kaetud tarkvara hoiustuse leppega ja et selle tarkvara ajakohasust tõendatakse regulaarselt;
- Interneti-rakenduste teostuseelses järgus küsitakse kolmandate poolte arvamust väljatöötamisele ja konfigureerimisele kuuluva turbearhitektuuri lahenduse hindamiseks.

7.2.8 Andmete kogumisel, analüüsimisel ja tõlgendamisel tuleks vajaduse korral ja kokkuleppel pangaga sobivalt kasutada andmeid või nõuandeid välistelt asjatundjatelt.

7.2.9 Järeldused ja soovitused peaksid põhinema andmete objektiivsel analüüsil ja tõlgendamisel.

7.2.10 Kogutud andmete, sooritatud analüüside, tehtud järelduste ja soovitatavate parandusmeetmete kohta tuleks säilitada kontrolljäljed ja neid kaitsta.

7.2.11 Enne aruande viimistlemist tuleks leidudele ja soovitustele saada vastavalt vajadusele kinnitus huvipooltelt, juhatuselt ja panga juhtkonnalt.

8 ARUANDLUS

8.1 Aruande sisu

8.1.2 IS audiitor peaks koostama regulaarseid aruandeid rakendatud tehnoloogiate, eeldatud riskide ja nende riskide käsitluse viiside kohta. Süsteemi soorituse seire on keskne edutegur. Sooritatud Interneti-panganduse läbivaatuse aruanne tuleks sõltuvalt läbivaatuse katvusest ja vastavalt vajadusele käsitleda alljärgnev:

- käsitlusala, eesmärgid, järgitud metoodika ja eeldused;
- Interneti-panganduse protsessi- või süsteemilahenduse üldine hinnang, väljendatult kesksete tugevate ja nõrkade kohtadena ning nõrkuste tõenäolise toimena;
- soovitused oluliste nõrkuste kõrvaldamiseks ja Interneti-panganduse protsessi- või süsteemilahenduse täiustamiseks;
- lausung panga eeskirjadele või kehtivatele seadustele vastavuse ulatuse ning kõigi lahknevuste toime kohta;
- lausung COBITi teabekriteeriumidele vastavuse ulatuse ning kõigi lahknevuste toime kohta;
- soovitused selle kohta, kuidas läbivaatuse õppetunde saaks ära kasutada analoogiliste tulevaste lahenduste või ürituste täiustamiseks.

G24 Interneti-pangandus (jätkub)

9 JÕUSTUMISKUUPÄEV

9.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. augustil 2003 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

LISA

Toetumine COBITile

Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

Interneti-panganduse läbivaatuse spetsiifilise auditiala puhul on kõige tõenäolisemalt asjakohased valitud plaanimise ja organiseerimise IT-protsessid, valitud hankimise ja evitamise IT-protsessid, valitud tarnimise ja toe IT-protsessid ja valitud seire ja hindamise IT-protsessid. Auditi sooritamisel tuleks seetõttu arvestada COBITi juhiseid alljärgnevate protsesside kohta.

- PO1 – Määratleda strateegiline IT plaan
- PO3 – Määrata tehnoloogiline suund
- PO8 – Tagada vastavus välisnõuetele (COBIT v3)
- PO9 – Hinnata IT riskid ja hallata neid
- HE2 – Hankida rakendustarkva ja hooldada seda
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE4 – Võimaldada käitus ja kasutamine
- HE5 – Hankida IT-ressursid
- HE6 – Hallata muutusi
- TT1 – Määratleda teenusetasemed ja hallata neid
- TT2 – Hallata kolmandate osapoolte teenuseid
- TT3 – Hallata suutlikkust ja võimsust
- TT4 – Tagada pidev teenus
- TT5 – Tagada süsteemide turvalisus
- TT8 – Hallata konsultatsioonipunkti ja intsidente
- TT10 – Hallata probleeme
- TT11 – Hallata andmeid

G24 Interneti-pangandus (jätkub)

- SH1 – Seirata ja hinnata IT töötulemusi
- SH2 – Seirata ja hinnata sisejuhtimist

Interneti-panganduse auditi puhul on kõige asjakohasemad teabekriteeriumid

- esmajärjekorras: konfidentsiaalsus, terviklus, käideldavus, vastavus ja usaldatavus;
- seejärel: toimivus ja tõhusus.

Allikad

Interneti-panganduse aabits. Chicago Föderaalreservi Pank, USA.

Baseli direktiiv nr. 82. Elektroonilise panganduse riskihalduse põhimõtted. Baseli pangandusjärelevalve komisjon. Šveits. Mai 2001.

Baseli direktiiv nr. 86. Tegevusriski halduse ja järelevalve usaldusväärsed tavad. Baseli pangandusjärelevalve komisjon. Šveits. Mai 2001.

Baseli direktiiv nr. 91. Elektroonilise panganduse riskihalduse põhimõtted. Baseli pangandusjärelevalve komisjon. Šveits. Juuli 2002.

BIS toimetised nr. 7. Elektrooniline rahandus: uued väljavaated ja uued jõuproovid. Rahvusvahelise arvelduse panga (BIS) rahandus- ja majandusosakond. Šveits. November 2001.

Cronin, M. J. Pangandus ja rahandus Internetis. USA: John Wiley & Sons, Inc. ISBN 0-471-29219-2.

Essinger, J. Virtuaalpanganduse revolutsioon. Ühendkuningriik: Thomson Business Press. ISBN 1-86152-343-2.

Interneti-panganduse riigikontrolöri käsiraamat. USA. Riigipankade rahahaldurite riigikontroll. Oktoober 1999.

Furst, K., Lang, W. W., Nolle, D. F. Interneti-pangandus: arengud ja väljavaated. Majandus- ja poliitikaanalüüsi töödokument 2000-9. USA. Rahanduskontrolliamet. September 2000.

Internet ja riigipanga osakond. USA. Riigipankade rahahaldurite riigikontroll. Jaanuar 2001..

Ühendkuningriigist kättesaadavate, kuid mitte Ühendkuningriigi investoritele mõeldud välismaistes Interneti veebisaitides oleva materjali käsitlemine. Ühendkuningriigi rahandusteenuste amet.

G25 Virtuaalsete privaatvõrkude läbivaatus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.2 Juhiseid annab suunis G16 "Kolmandate poolte mõju organisatsiooni IT-meetmetele".

1.1.3 Juhiseid annab suunis G17 "Auditivälise rolli mõju IS audiitori sõltumatusele".

1.2 Seos COBITiga

1.2.1 COBITi "Raamstruktuur" määrab: "Juhtkonna kohustus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste teostamiseks peab juhtkond rajama adekvaatse sisejuhtimissüsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- soorituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jäämise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusse indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

G25 Virtuaalsete privaatvõrkude läbivaatus (jätkub)

1.3 Suunise vajadus

1.3.1 Käesoleva suunise eesmärk on kirjeldada soovitatavaid tavasid virtuaalse privaatvõrgu (VPN) teostuste läbivaatuseks nii, et läbivaatuse kestel järgitaks asjassepuutuvaid IS auditeerimise standardeid.

2. VIRTUAALNE PRIVAATVÕRK (VPN)

2.1 Määratlus

2.1.1 IT Halduse Instituudi avaldatud dokument "Virtuaalne privaatvõrgustus. Uusi võrguturbeküsimusi" määratleb VPNi nii: "virtuaalkanalite võrk, mis kannab privaatliiklust läbi avalike või ühiskasutuslike võrkude, näiteks läbi Interneti või läbi võrguteenusetarnijate (NSPde) pakutavate võrkude". Käesoleva suunise otstarbeks kasutatakse seda VPNi määratlust.

2.1.2 VPNi kontekstis kasutatakse sageli termineid "tunnel" ja "tunneldus". Tunnelduseks nimetatakse protsessi, millega üht tüüpi pakett kapseldatakse teist tüüpi paketis, nii et andmeid saaks edastada selliste teede kaudu, mis muidu neid andmeid ei edastaks. Tunneliteks nimetatakse neid teid, mille kaudu kulgevad kapseldatud paketid Interneti VPNis.

2.2 VPNi mudelid

2.2.1 Kasutada saab VPNi kolme levinud mudelit. nende mudelite peamised erinevused on teenuse otspunktide ehk tunneliots punktide asukohas, vajalikus haldusetasemes, teenuse kvaliteedis ja sõltuvuses teenuseandja otsesest osalusest. Need kolm levinud mudelit on

- tarnijapõhine mudel,
- hübriidmudel,
- otspunktmudel.

2.2.2 Tarnijapõhises mudelis on enamik VPNi funktsioonidest ehitatud mitte organisatsiooni võrku, vaid teenusetarnija infrastruktuuri. Seda mudelit rakendatakse sageli ühe teenuseandja võrgu kaudu. Organisatsiooni võrgu ja teenusetarnija võrgu vahel on selge eraldusjoon. Kaugpääs organisatsiooni võrku antakse tavaliselt rendiliini (näiteks T1, T3) kaudu, ATM-ühendustega või Frame-Relay-eriühendustega. VPNiga seotud kaugpöörduse aparatuur ja tarkvara kuulub kliendile ja neid käitab klient, teenusetarnija võrgu sees asuv aparatuur ja tarkvara, alates väljuvast füüsilisest liinist kuulub teenusetarnijale ja neid käitab teenusetarnija. Teenusetarnija algatab võrgu piires asuvaid ja toetub mõlema otsa turbeks privaatliinidele. Selles mudelis on võrk ulatuslikult tarnija kontrolli all ning tarnija vastutab suutvuse plaanimise, kavandamise, konfigureerimise, diagnostika ja tõrkeotsingu eest.

2.2.3 Hübriidmudelis rakendatakse nii teenusetarnija võrku kui ka organisatsiooni võrku. VPN-tunnel algatatakse tarnija võrgust ja tunnel lõpetatakse organisatsiooni võrgus. Selles võrgus vastutab teenusetarnija kaugkasutajate VPN-tunnelite algatamise eest pärast kasutajate autentimist. Kui kaugkasutaja jõuab organisatsiooni võrguni, võidakse enne privaatvõrku pääsemise loa andmist nõuda teist autentimist. Kui kasutajad on autenditud, saavad nad pöörduda võrgu vahendite poole nii, nagu oleksid nad ühendatud otse ettevõtte kohtvõrguga.

2.2.4 Otspunktmudelis on teenusetarnijal ainult VPN-andmete transportija roll. Teenuse või tunnelduse otspunktiks võib olla töölaud või mingi VPN-seade, mis toimib mitme töölaua proksina. Teenuse mõlemad otspunktid on väljaspool teenusetarnija võrku. Seda mudelit saab kasutada kaugpöörduseks või mitme asukoha kokkuühendamiseks.

2.3 VPNi kasutamine

2.3.1 Sõltuvalt rakendatud mudelist saab VPNi kasutada mitmeti. Kõige tavalisemad kasutusotstarbed on

- mitme asukoha kokkuühendamine,
- kaugpöörduse ühendamine,
- ettevõtte laiendatud partnervõrgu (ekstraneti) ühendamine.

2.3.2 Mitme asukoha kokkuühendatavus võimaldab turvaliselt kokku ühendada eri sisevõrke, sisuliselt luua neist ühe suure sisevõrgu. Mitut asukohta ühendavaid VPNe kasutavad sageli geograafiliselt hajutatud organisatsioonid üheainsa loogilise võrgu loomiseks.

2.3.3 Kaugpöörduse ühendatavus võimaldab mobiilseil töötajail pääseda turvalise võrgusuhtluse abil Interneti kaudu oma organisatsiooni sisevõrku. Seda kasutatakse kombinatsioonis globaalse sissehelistusega, traadita ja lairibaedastusega Interneti-teenuste tarnijatega. Paljud organisatsioonid kasutavad kaugpääsu-VPNe odava võrkupääsu andmiseks oma töötajaile.

2.3.4 Ettevõtte laiendatud partnervõrgu ühendatavus võimaldab ühendusi võrkudega väljaspool ettevõtet. Seda võimalust kasutavad tihti äri-, teadus- või turunduspartnerid side kiirendamiseks turvaliste ühenduste kaudu. Üldiselt on partnervõrkudel tugevamad ohjemeetmed, mis võimaldavad lubada, hallata ja seirata võrkudevahelist liiklust ning sisevõrku võidakse partnervõrgu eest kaitsta tulemüüridega.

2.4 VPNi arhitektuur

2.4.1 VPNide installeerimiseks on palju võimalikke variante. Üks kõige tavalisemaid mooduseid organisatsiooni ühendamiseks Internetiga on võrguteenuste tarnija pakutav VPN. Ükskõik millises organisatsioonis võib VPNi arhitektuur olla üks järgmistest või nende kombinatsioon:

- tulemüüripõhised VPNid,
- marsruuteripõhised VPNid,
- kaugpöördusepõhised VPNid,
- riistvarapõhised ("musta kastiga") VPNid,
- tarkvarapõhised VPNid.

2.4.2 Tulemüüripõhised VPNid on kõige levinum teostusvorm. Kuna enamik organisatsioone kasutab juba niigi tulemüüre Internetiga ühendamiseks, tuleb neil lisada ainult krüpteerimistarkvara ja mingi volitamistarkvara.

2.4.3 Marsruuteripõhiseid VPNe on kahesuguseid. Ühtedes lisatakse marsruuterile krüpteerimise võimaldamiseks tarkvara. Teiste puhul tuleb marsruuteri paigaldusraamile paigaldada veel kolmanda poole tarnitav väline kaart, nii et krüpteerimist ei soorita enam marsruuteri protsessor, vaid see lisakaart.

2.4.4 Kaugpöördusepõhiste VPNide puhul saab keegi kaugasukohast luua krüpteeritud paketivoo või tunneli mingi organisatsioonis asuva võrguseadmeni.

2.4.5 Riistvarapõhiste ("musta kastiga") VPNide puhul pakub Tarnija VPN-tunneli loomiseks "musta kasti", st krüpteerimistarkvaraga seadet. Harilikult asub VPNi "must kast" andmeid kaitsva tulemüüri taga või tulemüüri kõrval, kuid VPNi süsteem võib tegelikult olla tulemüürist täiesti sõltumatu.

2.4.6 Tarkvarapõhistes VPNides hoolitseb tarkvara teise kliendini kulgeva tunnelduse ja pakettide krüpteerimise eest. Tarkvara laaditakse klienti ja serverisse. Liiklust alustab organisatsioonis asuv klient, mis loob ühenduse kaugasukohas paikneva serveriga. Kliendist väljuv liiklus krüpteeritakse või kapseldatakse ning marsruuditakse oma sihtkohta. Kui keegi püüab saada ühendust sisevõrguga, toimub see samal viisil.

2.5 VPNi konfiguratsioon ja topoloogia

2.5.1 VPNi konfigureerimisel tuleb seada võtme pikkuse, autentimisserverite, ühenduse ja jõudeoleku kontrollaegade, sertifikaadi genereerimise ning võtmete genereerimise ja jaotamise mehhanismide parameetrid. VPNi arhitektuuri konfigureerimiseks ja teostuseks ning arhitektuuri paigutamiseks VPNi topoloogiasse on mitmeid võimalusi. Organisatsioonidvõivad VPNi konfiguratsioonis kasutada üht järgnevaist kõige laiemalt kasutatavast topoloogiast või nende kombinatsiooni:

- tulemüür - klient,
- kohtvõrk - kohtvõrk,
- tulemüür - sisevõrk/partnervõrk,
- riistvara- ja tarkvara-VPN.

2.5.2 Tulemüür - klient on kõige laiemalt kasutatav topoloogia ning teda rakendatakse kaugkasutajate puhul, kes pöörduvad mingi sisevõrgu poole.

G25 Virtuaalsete privaatvõrkude läbivaatus (jätkub)

2.5.3 Kohtvõrk - kohtvõrk on teine kõige laiemalt kasutatav tehnoloogia. Kui kahe asukoha vahele on loodud tunnel, laiendab ta topoloogiat "tulemüür - klient" mitmesuguste kaugkontoriteni ning kontorite, äripartnerite ja tarnijate vahele.

2.5.4 Tulemüür - sisevõrk/partnervõrk: selles topoloogias kasutavad töötajad sisevõrke, väljastpoolt aga kasutavad kliendid, äripartnerid ja tarnijad partnervõrke. Kui kaugkasutajad püüavad pöörduda partnervõrgus või sisevõrgus olevate serverite poole, tuleb teha otsus, millistele serveritele neil tohib olla juurdepääs.

2.5.5 Riistvara- ja tarkvara-VPNid on autonoomsed seadmed, mis on määratud teostama VPNi tehnoloogia algoritme. Harilikult asub selline VPNi seade tulemüüri taga sisevõrgus. Andmepaketid kulgevad läbi tulemüüri ja VPNi seadme. Pakettide kulgemisel läbi nende seadmete saab neid krüpteerida. Tarkvaraga krüpteerimise mudelites, näiteks protokollis SSL, ei ole eriseadmeid (autentimiseks) üldiselt vaja ning paketivoo krüpteerib tarkvara.

2.5.6 VPNi tehnoloogiate ja protokollide hulka kuuluvad

- PPTP ("kakspunkt-tunnelduse protokoll"),
- L2TP ("kihi 2 tunnelduse protokoll"),
- IPSec ("turvaline Interneti protokoll"),
- SSL ("turvaline soklikiht").

3 VPNidega SEOTUD RISKID

3.1 Riskitüübid

3.1.1 Kuna VPN on ettevõtte side infrastruktuur, mis kasutab kolmanda poole teenuseid, võib temaga seotud riske liigitada nii:

- turvarisk,
- kolmandast poolest tulenev risk,
- äririsk,
- teostusrisk,
- käitusrisk.

3.2 Turvarisk ja õigusalane risk

3.2.1 VPNiga seotud turvariskde hulka kuuluvad järgmised:

- VPNide kasutamisest põhjustatud turvariskide ja õigusalaste riskide puudulik hindamine;
- ebapiisavad turbekavad infovaradele toimivate VPNidest põhjustatud riskide leevendamiseks;

- andmete puudulik kaitse enne nende sisenemist VPNi või nende väljumisel VPNist;
- mingi võrgutee kaudu kulgeva krüpteerimata teabe (sisemistes võrkudes enne krüpteerimisseadet, välistes võrkudes pärast krüpteerimisseadet) turbe ebaõnnestumine;
- teostuse puudumine, mis võib tekitada konfidentsiaalsuse, tervikluse, salgamise vääramise ja/või käideldavuse probleeme.

3.3 Kolmandast poolest tulenev risk

3.3.1 Sõltuvus kolmandast poolest võib tekitada selliseid riske:

- ebasobiva tarnija valimine,
- puudulik suhtehaldus,
- puudused teenusetasemelepetes (SLA) ja näitajad,
- ebasobiv juhtimise ja halduse protsess,
- SLAde ja näitajate puudulik mõõtmine ja seire,
- ebasobiv varundamise ja liiasuse strateegia,
- suhete ja teenuste ebapiisav mõõtlus;
- andmetele juurdepääsu väärkasutus VPNis.

3.4 Äririsk

3.4.1 Juhtkonna või ettevõtte ootused võivad jääda täitumata sellist tüüpi riskide tõttu:

- puudulik kooskõla äristrateegiaga,
- puudulik kulude säästmine,
- turvanõuete täitmata jäämine,
- ebapiisav kasutamise hõlpsus,
- kasutajate vajaduste rahuldamata jäämine sisu ja ulatuse poolest,
- teenuse kadu või halvenemine organisatsiooni või protsessi muudel aladel.

3.5 Teostusrisk

3.5.1 Järgmist tüüpi riskid võivad viia selleni, et teostatakse ebatoimiv ja ebatõhus lahendus:

- puudulik tähelepanu etteprojekteerimisele ja puudulik toetumine sellele;
- organisatsiooni jaoks ebasobiva VPNi mudeli valimine;

- puudulik kolmandate poolte kasutamine asjakohastel juhtudel;
- ebapiisav tähelepanu turvalisusele projekteerimisel;
- ebasobivad taasteprotsessid;
- teenusetaseme ootuste ja mõõtude kavandamata jätmine;
- ebasobiv integratsiooni strateegia;
- toimetu muutuse-, projekti- või teostusehalduse protsess;

VPNi kliendi risk (sama liides aktsepteerib Interneti ja VPNi liiklust).

3.6 Käitusrisk

3.6.1 Järgmist tüüpi riskid võivad viia selleni, et VPNi ärakasutus ja käitus on ebatoimiv ja ebatõhus:

- toimivaks käituseks piisamatud ressursid,
- usaldatavuse puudumine;
- teenuse kvaliteedi langus;
- koostalitlusvõime puudumine;
- kapselduse ebaõnnestumine;
- puudulik suutvus;
- liiasuse või varundamise puudumine;
- isiklike seadmete (koduarvutite) kasutamine tööalaseks otstarbeks (turvalise konfiguratsioonita, viirusetõrje tarkvarata, personaaltulemüürita);
- käitusparameetrite või andmete konfidentsiaalsuse puudumine.

4 PÕHIKIRI

4.1 Volitused

4.1.1 Enne VPNi läbivaatuse sooritamist peaks IS audiitor andma mõistliku kinnituse oma positsioonist tulenevate vajalike volituste kohta või saama kavandatud läbivaatuse sooritamiseks vajaliku kirjaliku volituse organisatsioonilt. Kui läbivaatuse algatas organisatsioon, peaks IS audiitor saama mõistliku kinnituse ka selle kohta, et organisatsioonil on asjakohane õigus seda läbivaatust toime panna.

G25 Virtuaalsete privaatvõrkude läbivaatus (jätkub)

5 SÕLTUMATUS

5.1 Kutsealane objektiivsus

5.1.1 Enne ülesande vastuvõtmist peaks IS audiitor andma mõistliku kinnituse selle kohta, et kui IS audiitoril on mingeid huve läbivaadatava VPNi lahenduse alal, ei kahjusta need mitte mingil viisil läbivaatuse objektiivsust. Igasuguse võimaliku huvide vastuolu puhul tuleks sellest selgelt teatada organisatsioonile ja enne ülesande vastuvõtmist tuleks saada kirjalik lausung selle kohta, et organisatsioon on vastuolust teadlik.

5.1.2 Kui IS audiitoril on või on olnud läbivaadatava VPNi alal mingeid auditiväliseid rolle, peaks ta arvestama suunist G17 "Auditivälise rolli mõju IS audiitori sõltumatusele".

6 PÄDEVUS

6.1 Oskused ja teadmised

6.1.1 IS audiitor peaks andma mõistliku kinnituse selle kohta, et tal on VPNi läbivaatuseks vajalikud tehnilised teadmised. VPNi teostuse läbivaatuseks organisatsioonis on vaja selgelt teada tegevusalaseid nõudeid ja VPNi tehnilisi aspekte.

6.1.2 IS audiitor peaks andma mõistliku kinnituse ka selle kohta, et tal on juurdepääs asjakohastele VPNi läbivaatuse sooritamiseks vajalikele tehnilistele oskustele ja teadmistele. VPNi läbivaatus nõuab häid tehnilisi teadmisi selliste aspektide hindamiseks nagu kasutatav krüpteerimistehnoloogia, võrguturbe arhitektuur ja turbe tehnoloogia. IS audiitoril peaksid olema adekvaatsed teadmised nende aspektide läbivaatuseks. Kui on vaja asjatundjate eriteavet, tuleks asjakohane teave hankida välistest kutsealastest ressurssidest. Väliste eriteadmisressursside kasutamise faktist tuleks organisatsioonile kirjalikult teatada.

7 PLAANIMINE

7.1 Jäme riski kaalutlemine

7.1.1 Jämedaks riski kaalutlemiseks peaks IS audiitor koguma teavet ettevõtte talitluse kohta ja sellest VPNile tulevate nõuete kohta.

7.1.2 VPNiga seotud riske, mis on loetletud alajaotises 3 ülal, tuleks arvestada sõltuvalt elutsükli järgust, milles läbivaatus sooritatakse, näiteks kavandamise ajal (teostuseelne), teostuse ajal või teostusjärgsena.

7.1.3 Tuleks välja selgitada ka asjassepuutuvad COBITi teabekriteeriumid (toimivus, tõhusus, konfidentsiaalsus, terviklus, käideldavus, vastavus, usaldatavus), mis on vaja läbi vaadata ja tõendada.

7.1.4 Selles kontekstis tuleks arvestada ka "Võrgukeskse tehnoloogia juhtimiseesmärke" (CONCT), sest see dokument laiendab COBITi kriteeriumid võrgukesksetele keskkondadele, näiteks sellistele, mida toetavad VPNid.

7.1.5 Selline jäme riski kaalutlemine aitab määrata läbivaatuse käsitlusala ja katvust.

7.2 Läbivaatuse käsitlusala ja eesmärgid

7.2.1 IS audiitor peaks (sobivatel juhtudel konsulteerides organisatsiooniga) selgelt määratlema VPNi läbivaatuse käsitlusala ja eesmärgi. Läbivaatusega hõlmatavad aspektid tuleks selgelt sõnastada käsitlusala ühe osana. Jaotises 7.1.1 viidatud jäme riski kaalutlemine dikteerib selle, millised aspektid tuleb läbi vaadata ning milline on läbivaatuse ulatus ja sügavus.

7.2.2 Läbivaatuse otstarbeks tuleks välja selgitada ja organisatsiooniga kokku leppida ka lahenduse huvipooled.

7.2.3 Läbivaatuse käsitlusalasse ja eesmärkidesse tuleks sobivatel juhtudel lülitada ka kõik huvipoolte kesksed probleemid.

7.2.4 Kui läbivaatuse käsitlusala hõlmab kolmandatest pooltest tarnijaid, peab IS audiitor veenduma, et auditiklausel sisaldub lepingus.

7.3 Metoodika

7.3.1 IS audiitor peaks sõnastama metoodika nii, et läbivaatuse käsitlusala ja eesmärke saaks saavutada objektiivsel ja professionaalsel viisil. Järgitav metoodika peaks sõltuma sellest, kas läbivaatus on teostuseelne, teostusaegne või teostusjärgne. Metoodika tuleks asjakohaselt dokumenteerida. Metoodika ühe osana tuleks spetsifitseerida ka see, millal ja kus kasutatakse väliste asjatundjate teavet. Metoodika ühe osana tuleks määrata ka igasugune kavasolev kontrollimis- või seirevahendite kasutamine.

7.4 Plaani kinnitamine

7.4.1 IS audiitor peaks vastavalt organisatsiooni tavadele saama plaanile ja metoodikale organisatsioonilt kooskõlastuse.

8 VPNi LÄBIVAATUSE SOORITAMINE

8.1 Üldist

8.1.1 See jaotis käsitleb laia aspektide spektrit, mida tuleb käsitleda VPNi läbivaatuse sooritamise ajal. Konkreetse VPNi läbivaatuse tarbeks tuleks vastavalt läbivaatuse kavandatud käsitlusalale ja eesmärkidele selles laias aspektide spektris piiritleda läbivaatuse seisukohalt asjassepuutuvad aspektid.

G25 Virtuaalsete privaatvõrkude läbivaatus (jätkub)

8.1.2 VPNi läbivaatus tuleks sooritada määratletud metoodika järgi (vajaduse korral seda detailiseerides), nii et läbivaatuse kavandatud eesmärgid saavutataks.

8.1.3 Andmete kogumisel, analüüsimisel ja tõlgendamisel tuleks üldiselt sobivalt kasutada kättesaadava dokumentatsiooni (äriplaan, süsteemi dokumentatsioon, lepingud, teenusetasemelepped ja logid) uurimist, vestlusi huvipoolte ja teenuseandjatega ning vaatlusi. Sobivatel juhtudel peaks IS audiitor kontrollima VPNi keskkonnas olulisi protsesse või funktsioone, tõendamaks, et need protsessid või funktsioonid töötavad kavatsetud viisil.

8.1.4 Andmete kogumisel, analüüsimisel ja tõlgendamisel tuleks sobivalt kasutada teavet välistelt asjatundjatelt, kui see on vajalik ja selle kohta on organisatsiooniga kokku lepitud.

8.1.5 Järeldused ja soovitused peaksid põhinema andmete objektiivsel analüüsil ja tõlgendamisel.

8.1.6 Kogutud andmete, tehtud analüüside, tulenevate järelduste ja soovitatud parandusmeetmete kohta tuleks säilitada asjakohaseid kontrolljälgi.

8.2 Teostuseelne läbivaatus

8.2.1 Teostuseelne läbivaatus, mis sooritatakse enne VPNi lahenduse teostamist (kavandamisjärgu ajal), peaks käsitlema seda, kui sobivad on

- nõuded VPNi lahendusele;
- pakutava lahenduse kulud ja tulud;
- pakutav VPNi tehnoloogia, näiteks VPNi mudel, VPNi arhitektuur, VPNi konfiguratsioon ja topoloogia, VPNi kasutusviis;
- pakutav turbearhitektuur ja turbefunktsioonid, sealhulgas pakutavad krüpteerimistehnoloogiad;
- kavandatud liiasus ja varundusvahendid;
- juhtkonnapoolsed kinnitused;
- pakutavad projektihalduse struktuurid ja seiremehhanismid;
- valimisprotsess teenuseandja valimiseks;
- pakutav leping, teenusetasemelepped ja mõõdustik;
- võimalikud põhikirja nõuded, mida tuleb täita.

8.2.2 Nende aspektide käsitlemiseks tuleks IS audiitoril

- uurida nõudeid VPNile, nii ärilisi kui ka tehnilisi;
- uurida äriplaani (kulusid ja tulusid) ja selle kinnitusi;
- vaadata läbi VPNi kavandamisdokument, mis visandab tehnoloogilised aspektid;
- vaadata läbi, kas pakutav lahendus vastab protokollile PPTP, L2TP või IPSec;

G25 Virtuaalsete privaatvõrkude läbivaatus (jätkub)

- vaadata läbi pakutav turbearhitektuur ja krüpteerimistehnoloogia;
- vaadata läbi pakkumisprotsess, sealhulgas alternatiivsete pakkumuste tehniline ja äriline hindamine ning lõplik teenuseandja valimine;
- uurida pakutavat projektihalduse struktuuri;
- uurida pakutavaid lepinguid, teenusetasemeleppeid ja mõõdustikke;
- uurida põhikirja nõudeid, mida tuleb täita;
- hinnata pakutavat liiasust ja varundusi;
- vaadata läbi pakutav strateegia VPNi integreerimiseks rakendustega;
- tehnoloogia ja turbe aspektide sobivuse hindamiseks kasutada vajaduse korral väliseid asjatundjaid;
- uurida pakutavaid koolitusplaane;
- uurida kõiki asjassepuutuvaid auditite ja läbivaatuste aruandeid;
- hinnata ülalloetletu tulemusi nende sobivuse seisukohalt ning nende adekvaatsust riskide (turvariski, kolmandatega seotud riski, äririski, teostusriski ja käitusriski) leevendamiseks;
- hinnata, kuidas on rahuldatud COBITi ja CONCT kriteeriumid;
- tõsta esile läbivaatusel ilmnenud riskid ja probleemid vajalike parandusmeetmete rakendamiseks.

8.3 Teostusaegne läbivaatus

8.3.1 Teostusaegne läbivaatus toimub teostamise ajal ja seetõttu peaks ta käsitlema seda, kas

- käimasolev teostus edeneb kinnitatud plaanide järgi ning kokkulepitud aegade ja kulude piires;
- VPNi tehnoloogia, st VPNi mudel, VPNi arhitektuur, VPNi konfiguratsioon ja topoloogia, VPNi kasutusviis, teostatakse nii, nagu kavatsetud;
- kasutatavad turbesüsteemid ja krüpteerimistehnoloogiad on stabiilsed ja vastavad kavandatule;
- kavandatud liiasus ja varundusvahendid teostatakse;
- tegelikud lepingud, teenusetasemelepped ja mõõdustik vastavad organisatsiooni nõuetele;
- kas võimalikud põhikirja nõuded täidetakse.

G25 Virtuaalsete privaatvõrkude läbivaatus (jätkub)

8.3.2 Ülalnimetatud aspektide käsitluseks tuleks IS audiitoril

- uurida projekti edenemise aruandeid ja nõupidamiste protokolle;
- hinnata tehnoloogia tegelikku teostust kavandatuga võrreldes ja tuvastada kõik lahknevused;
- teha kindlaks, kas on lahenduse vastavus protokollile PPTP, L2TP või IPSec on sertifitseeritud;
- hinnata turbearhitektuuri ja krüpteerimistehnoloogia tegeliku teostuse vastavust kinnitatud kavandile;
- uurida tegelikke lepinguid, teenusetasemeleppeid ja mõõdustikku kokkuleppelistega;
- hinnata loodud liiasust ja varundust;
- vaadata läbi VPNi tegelik integratsioon rakendustega;
- vajadusel kasutada väliseid asjatundjaid tegelikult teostatud tehnoloogia ja turvaaspektide sobivuse hindamiseks;
- hinnata testimise ja migratsiooni protsesside adekvaatsust, et otsustada, kas need arvestavad igat liiki kasutajaid ning katavad asjakohaselt suutvust, läbilaskevõimet, pääsu reguleerimist ja krüpteerimist;
- hinnata rajatavaid arvelduse mehhanisme;
- otsustada, kas VPNi teostuse edenemist mööda võetakse käigust pärilusühendused, katkestatakse nende arveldus ja kõrvaldatakse seadmed;
- uurida varasemat teostuseelse auditi aruannet, kui see on olemas, ja kõiki muid asjassepuutuvaid läbivaatuse aruandeid, et otsustada, kas varem soovitatud meetmed riski leevendamiseks on teostatud;
- hinnata ülalloetletu tulemusi nende sobivuse seisukohalt ning nende adekvaatsust riskide (turvariski, kolmandatega seotud riski, äririski, teostusriski ja käitusriski) leevendamiseks;
- hinnata, kuidas on rahuldatud COBITi ja CONCT kriteeriumid;
- tõsta esile läbivaatusel ilmnenud riskid ja probleemid vajalike parandusmeetmete rakendamiseks.

8.4 Teostusjärgne läbivaatus

8.4.1 Teostusjärgne läbivaatus toimub pärast VPNi teostamist ja seetõttu peaks ta selgitama, kas

- eeldatud hüvesid saadakse;
- ühekordsed kulud on plaanipärased ja mõistlikud;
- edasised arved on mõistlikud ja vastavad kokkuleppele;

G25 Virtuaalsete privaatvõrkude läbivaatus (jätkub)

- VPNi tehnoloogiat kasutatakse nii, nagu kavatsetud;
- VPN ja ta kasutamine vastab turvapoliitikatele ja -protseduuridele, sealhulgas andmete turvamäärangutele;
- partnervõrkude kaudu VPNi pääsevad kolmandad pooled on alla kirjutanud vastavatele turva- ja konfidentsiaalsuslepetele ning järgivad neid leppeid;
- kasutajad, kes saavad sülearvutite abil juurdepääsu kaugühenduse kaudu, kasutavad asjakohastel juhtudel vajalikke turbevahendeid, sealhulgas personaalseid tulemüüre;
- digitaalsertifikaatide halduseks on olemas asjakohased protsessid;
- teenusetasemeleppeid ja -näitajaid, sealhulgas teenuse kvaliteeti on õigeaegseks meetmete rakendamiseks regulaarselt mõõdetud, seiratud ja täiendatud;
- andmed on sisenemis- ja väljumispunktides ning krüpteerimata kanalites sobivate protseduuride abil piisavalt kaitstud;
- viirusetõrjeks, sissetungi avastamiseks jms otstarbeks on kasutusel sobivad turbevahendid ja -protsessid;
- teenused ja kulud on võrreldavad ja võistlusvõimelised;
- liiasus- ja varundusvahendid töötavad korralikult;
- võimalikud põhikirjalised nõuded täidetakse.

8.4.2 Ülalnimetatud aspektide käsitluseks tuleks IS audiitoril

- uurida projekti lõpparuannet;
- vaadata läbi tegelikus kasutuses olev VPNi tehnoloogia, et kontrollida selle vastavust kinnitatud kavandile;
- teha kindlaks, kas on lahenduse vastavus protokollile PPTP, L2TP või IPSec on sertifitseeritud;
- vaadata pisteliselt läbi regulaarsed arved;
- kontrollida pisteliselt vastavust turvapoliitikatele ja -protseduuridele;
- kontrollida kolmandate poolte juurdepääsu ning kolmandate poolte allakirjutatud leppeid partnervõrku pääsu kohta;
- kontrollida kaugpääsu ja sülearvutiga pääsu protsesse ning sobiva turvahäälestuse rakendamist sülearvutitel;
- vaadata läbi tegelikud teenusetasemelepped ja -näitajad, sealhulgas teenuse kvaliteet, ja nende seire tegelik protsess;
- kontrollida võrku läbiva turbe teostust;
- kontrollida varunduse ja liiasuse vahendeid;
- sooritada perioodilist mõõtlust mõistliku kinnituse saamiseks arvete ja teenusekvaliteedi pideva mõistlikkuse kohta;

- vajadusel kasutada rakendatud tehnoloogia ja turbeaspektide sobivuse hindamiseks väliseid asjatundjaid;
- kasutada sobivaid vahendeid VPNi lahenduse asjassepuutuvate aspektide kontrollimiseks;
- vaadata läbi VPNi toetav konsultatsioonipunkti protsess;
- hinnata ülalloetletu tulemusi nende sobivuse seisukohalt ning nende adekvaatsust riskide (turvariski, kolmandatega seotud riski, äririski, teostusriski ja käitusriski) leevendamiseks;
- hinnata, kuidas on rahuldatud COBITi ja CONCT kriteeriumid;
- tõsta esile läbivaatusel ilmnenud riskid ja probleemid vajalike parandusmeetmete rakendamiseks.

9 ARUANDLUS

9.1 Aruande sisu

9.1.1 VPNi läbivaatuse aruandes peaksid sõltuvalt läbivaatuse katvusest olema käsitletud järgmised aspektid:

- käsitlusala, eesmärk, järgitav metoodika ja eeldused;
- lahenduse üldine hinnang väljendatuna kesksete tugevate ja nõrkade külgede ning nõrkuste tõenäoliste mõjude kaudu;
- soovitused oluliste nõrkuste kõrvaldamiseks ja lahenduse täiustamiseks;
- COBITi teabekriteeriumidele ja CONCT kriteeriumidele vastavuse ulatus ja kõigi lahknevuste toime;
- soovitused saadud kogemuste kasutamiseks analoogiliste tulevaste lahenduste või ürituste täiustamiseks.

9.1.2 Enne aruande lõpetamist tuleks leiud ja soovitused vastavalt vajadusele kooskõlastada huvipooltega ja organisatsiooniga.

10 JÄRELTOIMINGUD

10.1 Kokkulepitud meetmete jälgimine

10.1.1 VPNi läbivaatuse lõpetamisel kokkulepitud toimingutele tuleks määrata tähtpäevad ja neid tuleks jälgida nende lõpuleviimiseni. Lahendamata jäänud küsimuste käsitlusse tuleks vajalike meetmete rakendamiseks kaasata asjakohane juhtkond.

G25 Virtuaalsete privaatvõrkude läbivaatus (jätkub)

11 JÕUSTUMISKUUPÄEV

11.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. juulil 2004 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

LISA

Toetumine COBITile

Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi protsesside valimise põhjal ja arvestades COBITi teabekriteeriume.

VPNi kui side infrastruktuuri puhul on asjakohasemad alljärgnevad aspektid.

- PO1 – Määratleda strateegiline IT plaan
- PO3 – Määrata tehnoloogiline suund
- PO5 – Hallata IT-investeeringuid
- PO8 – Tagada vastavus välisnõuetele (COBIT v3)
- PO9 – Hinnata IT riskid ja hallata neid
- PO10 – Hallata projekte
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE4 – Võimaldada käitus ja kasutamine
- HE5 – Hankida IT-ressursid
- HE6 – Hallata muutusi
- TT1 – Määratleda teenusetasemed ja hallata neid
- TT2 – Hallata kolmandate osapoolte teenuseid
- TT3 – Hallata suutlikkust ja võimsust
- TT4 – Tagada pidev teenus
- TT5 – Tagada süsteemide turvalisus
- TT9 – Hallata konfiguratsiooni
- TT12 – Hallata füüsilist keskkonda
- TT13 – Hallata käitust
- SH1 – Seirata ja hinnata IT töötulemusi

G25 Virtuaalsete privaatvõrkude läbivaatus (jätkub)

VPNi läbivaatuse puhul on kõige asjakohasemad teabekriteeriumid

- esmajärjekorras: käideldavus, konfidentsiaalsus, toimivus ja terviklus;
- teises järjekorras: tõhusus, vastavus ja usaldatavus.

Viidatud allikad

Virtuaalsed privaatvõrgud. Uusi võrguturbe küsimusi. IT Halduse Instituut, USA. 2001.

Võrgukeskse tehnoloogia juhtimiseesmärgid (CONCT). IT Halduse Instituut, USA. 1999.

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.2 Juhiseid annab suunis G17 "Auditivälise rolli mõju IS audiitori sõltumatusele".

1.1.3 Juhiseid annab suunis G21 "Ettevõtte ressursside plaanimise (ERP) süsteemide läbivaatus"

1.2 Seos COBITiga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- soorituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jäämise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusse indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

1.3 Suunise vajadus

1.3.2 Tootmis- ja teenindusorganisatsioonid on oma arengu toetamiseks dünaamilises ja kiiresti muutuvas ärikeskkonnas üha enam huvitatud äriprotsesside ümberrajamisest (BPR). BPR pakub hinnalist võimalust saavutada äritulemustes tõelist murrangut, kuid ta toob kaasa ka riske, näiteks siis, kui tehakse väärad ümberrajamise valikud või kui kavandatud muudatused teostatakse ebaadekvaatselt.

1.3.3 Ümberrajamine tähendab laialdasi muudatusi mitte ainult äriprotsessides, vaid ka juhtimis- ja abistruktuurides, inimestes ja organisatsioonis, tehnoloogias ja infosüsteemides ning poliitikates ja eeskirjades. See tähendab, et BPR-projektid mõjutavad tugevalt nende organisatsioonide juhtimissüsteemi, kes on teostanud ümberrajamise. Konkreetsemalt, on suurenenud risk, et protsessi ümberrajamisel on äritehingute kiirendamiseks välja jäetud olulised turvameetmed. Seetõttu tuleks IS audiitor olla sellest teadlik ja sisendama juhtkonnale, et turvameetmed tunduvad küll oma loomult protsessi aeglustavatena, kuid nad on möödapääsmatud sellise riski vältimiseks, mille tõenäosust ega toimet ei ole hõlbus hallata või mõõta.

1.3.4 Käesoleva suunise eesmärk on anda IS audiitoritele põhiliste ümberrajamise probleemide kujul raamstruktuur, millega kaalutleda keskseid BPR-pojektidega seotud ülesandeid ja riske, pöörates tähelepanu eriti IS aspektidele.

2 ÄRIPROTSESSIDE ÜMBERRAJAMISE PROJEKTID

2.1 Määratlus

2.1.1 Äriprotsesside ümberrajamise mingit üldtunnustatud määratlust küll ei ole, kuid kõige sagedamini tsiteeritakse Hammeri ja Champy pakutud määratlust: äriprotsesside põhjapanev uuesti läbimõtlemine ja radikaalne ümberkujundamine oluliste nüüdisaegsete sooritusmõõtude, näiteks kulude, kvaliteedi, teenuse ja kiiruse tunduva paranemise saavutamiseks. [1]

2.1.2 BPR eesmärk on täiustada äriprotsesse nende struktuuri põhjaliku läbivaatuse teel ning järsult muutes protsesside haldamise ja teostamise viisi. Harilikult avaldab see tugevat mõju osalevatele inimestele ning töötavadele ja abitehnoloogiatele, eriti infotehnoloogiatele.

2.2 BPR peamised tulemused

2.2.1 BPR-projekt on äärmiselt kõikjaletungiv. Tema toimel muutuvad oluliselt kõik organisatsiooni protsessid ja seosed. BPR-projekti peamised tulemused võib seega võtta kokku järgmiselt:

- kontseptsioonilt strateegiline;
- uued äriprioriteedid põhinevad väärtusel ja kliendi nõuetel (kliendikeskne, tulemile keskendatud), rõhk on protsessil (eelkõige kesksetel äriprotsessidel) kui toote, teenuse ja kasumlikkuse täiustamise vahendil;

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

[1] Hammer ja Champy. Korporatsiooni ümberrajamine. 1993.

- uued lähenemisviisid inimeste organiseerimisele ja motiveerimisele ettevõttes ja väljaspool;
- uued lähenemisviisid tehnoloogia kasutamisele kaupade ja teenuste väljatöötamiseks, valmistuseks ja väljastuseks;
- tarnijate rollide ümbermääratlemine, mis hõlmab väljasttellimist, ühisarendust, viivituseta ladustust ja tuge;
- klientide ja tarbijate rollide ümbermääratlemine, mis võimaldab neil otsesemalt ja aktiivsemalt osaleda ettevõtte äriprotsessides.

2.3 BPR põhimõtted ja tegevused

2.3.1 Põhimõtted abistavad uuenduslikku mõtlemist, mis on vajalik protsessi struktuuri muutmiseks. Põhimõtetest on kasu peamiselt protsessi muutmise võimaluste kaalutlemisel; tavaliselt on see BPR-projektide kõige raskem järk.

2.3.2 Hammer soovitas järgmisi BPR põhimõtteid:

- mitu ametikohta ühendatakse;
- töötajad teevad otsuseid;
- protsessi sammud sooritatakse loomulikus järjestuses;
- protsessidel on mitu versiooni;
- töö sooritatakse seal, kus see on kõige mõttekam;
- kontrollide ja meetmete arv on väiksem (kuid väga tähtsad on teostusele rakendatavad meetmed);
- lahknevuste reguleerimine on minimaalne;
- ainsaks kontaktpunktiks on juhtumihaldur;
- valdavad on tsentraliseeritud ja detsentraliseeritud operatsioonide hübriidid.

2.3.3 Teised, sealhulgas Carter ja Handfield, soovitavad BPR tegevused viia läbi sellises järjestuses: 1) lihtsustamine (mis sisaldab mitteväärindavate tegevuste kõrvaldamist), 2) standardimine, 3) integreerimine, 4) parallelism, 5) varieeruvuse ohje, 6) ressursside jaotamine, 7) automatiseerimine. Nad osutavad, et BPR-protsess peaks läbima sammud 1 kuni 7 ranges järjestuses. Näiteks oleks väär püüda automatiseerida mingit protsessi IT-rakendusega, ilma et kõigepealt mõeldaks ta lihtsustamisele; lihtsustamine võib muuta automatiseerimise liigseks, kuid ka automatiseerimise täielikud hüved võivad jääda realiseerimata. Mõtlemisprotsessi kitsendamine range järjestusega on aga ka ohtlik. Näiteks võib mitmesuguseid ressursse nõudvate tegevuste integreerimine üheks tegevuseks, mille sooritab üks inimene, mõnikord saada võimalikuks ainult automatiseerimisega.

2.3.4 Mõnikord on parimaks lähenemisviisiks holistlik (terviksüsteemne).

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

2.4 BPR metoodika

2.4.1 Ümberrajamine on olemuslikult väga situatsiooniline ja loov. Kirjandusest võib leida põhiliselt kaks lähenemisviisi BPRile.

2.4.2 Algselt Hammeri ja Champy pakutud metoodika on laskuv metoodika, mis soovitab BPR-rühmal keskenduda otsustamisele, kuidas võib saavutada organisatsiooni strateegilised eesmärgid, laskmata oma mõtlemist kitsendada olemasoleva protsessiga. Rõhk on sihtprotsessil ja on kooskõlas samm-muutuse filosoofial, mida esindavad autorid.

2.4.3 Harringtoni visandatud inkrementaalsem metoodika on ülenev metoodika, mis soovitab modelleerida olemasolevat protsessi selle tundmaõppimiseks, seejärel aga muuta seda strateegiliste eesmärkide saavutamiseks sobivalt sujuvamaks. Keskendutakse senise protsessi muutmisele, selgitades välja võimalusi selle täiustamiseks.

2.4.4 Praktikas tuleb BPR-rühmal harilikult kasutada segametoodikat. Kui aluseks võetakse laskuv metoodika, tuleb ikkagi tunda seniseid funktsioone ja hoolikalt määratleda siirdetee senisest protsessist tulevase eelistatava protsessini. Üleneva metoodika puhul võivad BPR-rühmad kulutada liiga palju aega olemasoleva protsessi detailiseerimisele ja kaotada uuendusliku mõtlemise. Segametoodika õhutaks rühma mõtlema üldtaseme muudatustele, koormamata end senise protsessi üksikasjadega.

2.4.5 Tähtis on mõista, et algne BPR uuring võib viia soovitusteni käivitada rida detailsemaid projekte alamprotsesside täiustamiseks, mis võib nõuda ainult suhteliselt väikesi muudatusi (võib-olla mõnede kitsaskohtade kõrvaldamiseks).

2.5 Mitme BPR metoodika kuus põhisammu

2.5.1 Nägemuse loomine. Tavaliselt saavutab BPR-projekti eestvedaja selles järgus tippjuhtkonna toetuse. Kõrgemaid juhte ja firma protsesside tundjaid sisaldavale töökonnale antakse volitused võtta vaatluse alla mingi äriprotsess selle täiustamiseks äristrateegia ja IT võimaluste läbivaatuse põhjal, lootes muuta paremaks firma üldisi töötulemusi.

2.5.2 Algatamine. See järk sisaldab ümberrajamise projektirühma määramist, tulemuste sihtide seadmist, projekti plaanimist ning huvipoolte ja töötajate teavitamist ja kaasatõmbamist. Sageli saavutatakse see ümberrajamise äriplaani koostamisega mõõtluse, väliste klientide vajaduste väljaselgitamise ja tasuvusanalüüsi põhjal.

2.5.3 Diagnoosimine. See järk kujutab endast senise protsessi ja ta alamprotsesside dokumenteerimist protsessiatribuutide, näiteks tegevuste, ressursside, suhtluse, rollide, IS ja maksumuse väljenduses. Protsessinõuete tuvastamisel ja kliendiväärtuse kinnistamisel tuvastatakse ilmnevate probleemide ja mitteväärindavate tegevuste algpõhjused.

2.5.4 Ümberkujundamine. Ümberkujundamise järgus töötatakse välja uus protsessi lahendus. Seda tehakse protsessi lahenduse alternatiivide kavandamisega ajurünnaku ja loomemeetoditega. Uus lahendus peaks vastama strateegilistele eesmärkidele ning sobima inimressursi ja IS arhitektuuridega. Tavaliselt sooritatakse uue protsessi dokumenteerimine ja prototüüpimine ning viiakse lõpule uut protsessi toetavate uute infosüsteemide kavandamine.

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

2.5.5 Rekonstrueerimine. See järk toetub tugevalt muutusehalduse meetoditele, millega võib saada mõistliku kinnituse sellele, et üleminek uutele kohustustele protsessi alal ja inimressursi rollidele on sujuv. Selles järgus teostatakse IT-platvorm ja -süsteemid ning kasutajad läbivad koolituse ja üleviimise.

2.5.6 Hindamine. BPR metoodika viimane järk nõuab uue protsessi seiret ta sihtide saavutatuse määramiseks ning sageli sisaldab sidet täieliku kvaliteediprogrammiga.

2.6 BPR instrumendid

2.6.1 BPR ettevõtvail organisatsioonidel võib olla palju kasu sobivatest BPR instrumentidest, mis aitavad vähendada BPR riske. Nii senise kui ka uue äriprotsessi puhul toetab tüüpiline BPR instrument protsessi modelleerimist, analüüsi ja hindamist ning ta tõenäolise käitumise simuleerimist.

2.6.2 Kuna diagnostikajärku (2.5.3) loetakse tegevustulemuste täiustusvõimaluste ja takistuste tuvastuse võtmeks, etendavad BPR projektis tähtsat rolli BPR instrumendid. IS audiitor peab läbi vaatama ka need instrumendid.

2.7 IS roll BPRis

2.7.1 IS annab instrumendid ja mängib BPR projektides nelja eri rolli.

2.7.2 IS võimaldab uusi protsesse. IS võib aidata kavandada uuenduslikke äriprotsesse, mis ei oleks muidu teostatavad. IS võib olla keskne BPR võimaldaja. IT kasutamine paneb kahtlema eeldustes, mis on loomuomased sellistele tööprotsessidele, mis on olemas olnud juba ammu enne nüüdisaegsete IT-rakenduste ilmumist. BPR juured võivad küll olla IS halduses, kuid ta on eelkõige äriline üritus, millel on laialdased tagajärjed klientide vajaduste ja organisatsiooni muude koostisosade vajaduste seisukohalt.

2.7.3 IT-vahendid aitavad hõlbustada projektihaldust. Projektihalduse vahendid aitavad analüüsida protsesse ja määratleda uusi protsesse. Nende abil saab määratleda ka protsessikesksete rakendustarkvara pakettide kasutuselevõttu.

2.7.4 IS võimaldab inimestel tihedamalt koos töötada. IS üha tungivama rolli elemendid on eritarkvara süsteemid, näiteks elektronpost, rühmvara, töövoo haldus ja kaugnõupidamine.

2.7.5 IS aitab integreerida äritegevusi. Äritegevuste protsessivaade hõlmab äriprotsesside integreerimist ettevõttes ja ka äripartnerite hulgas. ERP süsteemid on täielikult integreeritud ja aitavad kehtestada ümberrajamise protsessi, keskendudes BPR teostamise protsessile.

2.8 BPR projektide riskid

2.8.1 Radikaalselt täiustatud äriprotsessid võivad senisest paremini rahuldada klientide nõudeid ja võivad järsult parandada organisatsiooni tegevustulemusi. Järsud paranemised aga ei teki riskideta ega sagedate tõrgeteta. Ümberrajamise hüvesid ei saada tingimata õigeks ajaks. See tähendab, et BPR projekte tuleb projekti elutsükli kestel hoolikalt seirata.

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

2.8.2 Muutmisprotsessi igal sammul (kavandamisel, teostamisel, käikuandmisel) võib tekkida probleeme, mis on seotud sponsorluse, käsitlusala, organisatsioonilise kultuuri, eestvedamise, oskuste, inimressursside ja juhtimisega. Näited probleemide tüüpide kohta on kokku võetud järgnevas.

2.8.3 Kavandamisriskide hulka kuuluvad

- sponsorluse probleemid:
  - tegevjuhataja ei toeta,
  - tippjuhtkonna kohustumus ei ole piisav,
  - juhtkonna skepsis,
  - üritust juhib väär tegevjuht,
  - kavandamisrühmas on väärad liikmed,
  - puudulik olulisuse teatamine;
- käsitlusala probleemid:
  - puudub seos strateegilise nägemusega,
  - käsitlusala on liiga kitsas või liiga ambitsioonikas,
  - "pühade lehmade" kaitsmine,
  - seniste ametikohtade kaitsmine,
  - analüüsihalvatus;
- oskuste probleemid:
  - puudulik uute ideede uurimine,
  - spontaanse mõtlemise puudumine,
  - suletus uutele ideedele,
  - kavandamise väärad kontseptsioonid,
  - kultuurimuutus ei ole organisatsioonile kohandatud,
  - inimressursiküsimuste puudulik arvestamine,
  - IS-talituse toetusvõime ületamine;
- poliitikaprobleemid:
  - võimu kaotavate juhtide sabotaaž,
  - lammutav kriitika,
  - stiihilised kuulujutud,
  - muutuste kartus,
  - kultuuriline vastuseis.

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

2.8.4 Teostusriskide hulka kuuluvad

- juhatamisprobleemid:
  - tippjuhtkonna puudulik tähelepanu, kohustumus või mõju,
  - omandusvõitlus,
  - tegevjuhataja või sponsori kõikuv või nõrk poliitiline tahe,
  - tegevjuhataja või sponsori vahetumine,
  - puudulikud ressursid,
  - ei suudeta edasi anda veenvat nägemust,
  - tegevjuhataja ei suuda ühendada juhtkonda üritust toetama;
- tehnilised probleemid:
  - IT teostusvõime ületamine,
  - tarkvara teostuse hilinemine,
  - valmistarkvara puudulik suutvus,
  - funktsionaal- ja lahendusnõuete probleemid,
  - olulised küsimused pole algselt välja selgitatud,
  - keerukuse alahindamine,
  - käsitlusala ettenägematu muutumine,
  - aeganõudvad või kulukad arendusstrateegiad;
- siirdeprobleemid:
  - kavandamisjärgu kesksete töötajate kaotamine,
  - hoo kaotamine,
  - töötajate kurnatus,
  - käsitlusala probleemid,
  - oodatuist aeglasemad tulemused,
  - eelarve ülekulud,
  - ebarealistlikud tähtajad,
  - algse käsitlusala kitsenemine,
  - inimressursiküsimuste hooletussejätt,
  - üritus nõuab liiga suurt pingutust.

2.8.5 Käitus- ja käikuandmisriskide hulka kuuluvad

- kultuuri ja inimressursiprobleemid:
  - kultuurilise vastuseisu kasv,
  - ebaotstarbekas käitumine ei vähene,

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

- omaksvõtu puudumine viib eeldatud hüvede murenemiseni;
- puudulik või edutu koolitus,
- tulemused ei vasta lubadustele või üldisele ettekujutusele;

- juhtimisprobleemid:
  - uute juhtimisoskuste edutu rakendamine,
  - ei hoolitseta pideva täiustamise tegevuste eest,
  - omanduse, mõjualade ja võimu küsimused pole rahuldavalt lahendatud,
  - ilmnenud probleemide ületamiseks ei piisa tahet,
  - nõrk suhtlus,
  - töötajate ja juhtide aktiivne või passiivne sabotaaž;
- tehnilised probleemid:
  - tugi hilineb ja/või on halb,
  - süsteemi- või tarkvaravigadest tingitud käitusprobleemid,
  - süsteemid ei vasta kasutajate vajadustele või ootustele,
  - puudulik testimine,
  - andmetervikluse probleemid õõnestavad usaldust.

3 AUDITITALITUSE PÕHIKIRI

3.1 Muudatused BPR-projektide puhuks

3.1.1 Kui organisatsioon on otsustanud teostada BPR projekte, on võib-olla vaja muuta IS auditi talituse põhikirja. BPR kaalutlused nõuavad IS audiitori töö käsitlusala või suhteid teiste audititalitustega (näiteks rahandusliku või tegevusalasega) laiendataks ja tihedamalt integreeritaks.

3.1.2 On möödapääsmatu, et organisatsiooni kõrgem juhtkond ja süsteemijuhtkond täielikult tunneks ja toetaks IS audiitori rolli (rolle), mis on seotud BPR projektiga. IS auditeerimise suunis G5 "Audititalituse põhikiri" tuleks läbi vaadata ja arvesse võtta organisatsiooni BPR projektide ning nendega seotud ürituste kontekstis.

4 SÕLTUMATUS

4.1 IS auditi rollid BPR projektides

4.1.1 Kui IS audiitoril tuleb täita BPR projektidega seotud auditiväliseid rolle või nende eest vastutada, tuleks läbi vaadata IS auditeerimise suunis G17 "Auditivälise rolli mõju IS audiitori sõltumatusele" ja seda asjakohaselt järgida.

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

4.1.2 Kui IS audiitoril tuleb BPR projektis täita auditivälist rolli, peaks ta läbi vaatama ka ISACA standardid infosüsteemide juhtimise spetsialistidele ning neid asjakohaselt järgima.

4.1.3 Ülalnimetatu põhjus on selles, et niisugused asjaolud väga tõenäoliselt kahjustavad IS audiitori sõltumatust. Konkreetsemalt, IS audiitor peaks keelduma läbi vaatamast selliseid süsteeme, protseduure või protsesse, mis allutatakse BPRile ja mille puhul IS audiitor kuulus BPR töörühma koosseisu.

5 PÄDEVUS

5.1 Vajalikud ärialased teadmised ja tehnilised oskused

5.1.1 Oma teadmiste tõttu süsteemide ja meetmete alal võivad IS audiitorid kesksete äriprotsesside ümberrajamisel mängida väga olulist rolli, ehkki neil tuleb oma oskusi ja auditi metoodikat ümber kujundada, sest mõndagi sellest, mida IS audiitorid on harjunud protsessidest leidma, on mõjutanud või kõrvaldanud BPR radikaalsed muudatused.

5.1.2 BPR projekti auditeerimisel on IS audiitor harilikult üks komponente auditirühmas, kus ta täiendab teiste (rahanduse, tegevusala, regulatsiooni) audiitorite oskusi oma oskustega IS alal. IS audiitor peaks aga veenduma, et tal on BPR projekti läbivaatuseks vajalikud teadmised äritegevuse alal. IS audiitor peaks ka andma mõistliku kinnituse sellele, et tal on juurdepääs BPR projekti läbivaatuse sooritamiseks asjassepuutuvatele tehnilistele oskustele ja teadmistele.

6 PLAANIMINE

6.1 Raamstruktuur, mida IS audiitor peaks arvestama BPR projekti läbivaatamisel

6.1.1 Algatusjärgus ja diagnostikajärgus analüüsitakse seniseid protsesse, teavet ja kasutuselolevaid IT-süsteeme ning võrreldakse neid mõõtluse teel teiste süsteemidega. Sel ajal saab IS audiitor mõõta iga uurimiseks valitud protsessi asjassepuutuvaid hetke sooritusnäitajaid ja selgitada välja sooritusse puudused. Kuna teabe ja IT kasutamine võib olla organisatsiooni protsesside järskude muudatuste hoovaks, saab IS audiitor anda kasulikke panuseid juba alates BPR protsessi algjärkudest.

6.1.2 Ümberkujundamise järgus kavandatakse uued protsessid, otsitakse uut teavet või senise teabe uusi kasutusviise, määratletakse uue ärisüsteemi kavand, töötatakse välja ülemineku strateegia ja luuakse ülemineku tegevusplaan. IS audiitor võib läbi vaadata uue töövoo sihtmudeli, uue teabe ühiskasutuse viisi ettevõtte tegevusliinide vahel, IT-süsteemide ümberkujundamise, uue teabe ja uute tehnoloogiate kasutuselevõtu, vana teabe ja vanade IT.süsteemide kõrvaldamise viisi ning uue juhtimissüsteemi usaldatavuse.

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

6.1.3 Hindamisjärgu ajal on uued protsessid ja infosüsteemid kasutusel. IS audiitori spetsiifiline ülesanne on teha kindlaks, kas BPR projekt on oma sihid saavutanud, kas üleminek uuele struktuurile on toimiv ja usaldatav ning kas täielik kvaliteediprogramm on aktiveeritud.

7 AUDITITÖÖ SOORITAMINE

7.1 Riskihalduse hindamine

7.1.1 Kuna ümberrajamine on olemuslikult väga situatsiooniline ja loov (ei ole olemas mingit ainuõiget viisi, kuidas seda teha), on kirjanduses mitu BPR protseduuri. BPR projekti audit ei saa olla mingile metoodikale vastavuse audit, vaid ta hindab riskihaldust ning seda, kuidas saavutatakse lõplikud tulemuste paranemised, mis on olulised klientidele ja huvipooltele.

8 ARUANDLUS

8.1 Aruande sisu

8.1.1 BPR läbivaatustes tuleks aruandlust sooritada sedamööda, kuidas tuvastatakse riske ja probleeme. Need aruanded tuleks meetmete rakendamiseks adresseerida asjakohasele juhtkonnale. Võib koostada lõpparuande, mis loetleb kõik läbivaatuse käigus tõstatatud küsimused.

8.1.2 Sõltuvalt läbivaatuse tüübist peaks aruanne käsitlema näiteks järgmisi aspekte:

- BPR lähenemisviisi mudeli ja metoodika sobivus,
- riskid ja probleemid, nende põhjused ja toime,
- võimalikud riski leevendamise meetmed,
- kulude ja tulude võrdlus ning mõju organisatsiooni keskkonnale.

9 JÕUSTUMISKUUPÄEV

9.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. juulil 2004 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

LISA

Viidatud allikad

- Carter, M., Handfield, R. Identifying Sources of Cycle-time Reduction. Reengineering for Time-based Competition. Quorum Books, 1994.
- Hammer, M., Champy, J. Reengineering the Corporation: A Manifesto for Business Revolution. Harper-Collins, USA, 1993.
- Harrington, H.J. Business Process Improvement. McGraw-Hill, USA, 1991.

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

BPR vahendid ja meetodid

Rida vahendeid ja meetodeid on välja töötatud spetsiaalselt protsessiteadmuse hõiveks ja esituseks, kuid ümberrajamise uuringute tarbeks loetakse kasulikeks ka mitmeid juba olemasolevaid vahendeid ja meetodeid. Sama protsessi eri vaated võivad mõneti aidata protsessi tundma õppida, kuid harilikult ei tugevda nad uuendusliku mõtlemise vajadust. Vahendid ja meetodid võib üldjoontes liigitada järgmistesse klassidesse.

- SSM (*soft systems methods*, "leebed süsteemimeetodid"). Need on kvalitatiivsed ja/või ajurünnakmeetodid mõtlemisprotsessi formaliseerimiseks ja nende sagedad kasutusalad on

  - protsessi või süsteemi sihtide seadmine;

  - probleemianalüüs, näiteks protsessi tõrke põhjuste tuvastamiseks (näiteks põhjuste ja tagajärgede skeemiga);

  - riskianalüüs.

- Esitusvahendid. Need on protsessi vaadete esituse meetodid senise või pakutava uue protsessi tundmaõppimiseks ja seletamiseks. Näiteid:

  - rollitegevuste skeemid, mis näitavad isikute, töörühmade või allüksuste vahelisi sõltuvusi protsessis;

  - protsessi voodiagrammid, mis näitavad tegevuste vahelisi sõltuvusi;

  - funktsionaalse dekompositsiooni mudelid, mis on kasulikud infosõltuvuste näitamiseks;

  - ajapõhine protsessi vastendus, millega esitatakse protsessi sooritusaja dekompositsioon väärindavateks ja mitteväärindavateks komponentideks protsessi eri järkudes.

- Analüüsivahendid. Neid vahendeid saab kasutada protsessi käitumise uurimiseks ajas. On olemas mitmesuguseid vahendeid modelleerimisvõime eri tasemetel, näiteks PERT/CPM, Petri võrgud ja diskreetsündmustega simuleerimine.

IS audiitor peaks olema teadlik riskist ülemäära toetuda senise protsessi modelleerimisele: see võib hakata asendama tegelikke otsuseid.

Toetumine COBITile

Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ja arvestades COBITi teabekriteeriume.

Protseduur on seotud järgmiste COBITi primaarprotsessidega.

- SH1 – Seirata ja hinnata IT töötulemusi
- SH2 – Seirata ja hinnata sisejuhtimist
- TT1 – Määratleda teenusetasemed ja hallata neid
- TT10 – Hallata probleeme

G26 Äriprotsessi ümberrajamise (BPR) projekti läbivaatus (jätkub)

- HE6 – Hallata muutusi
- PO1 – Määratleda strateegiline IT plaan
- PO9 – Hinnata IT riskid ja hallata neid
- PO10 – Hallata projekte

Protseduur on seotud järgmiste COBITi protsessidega

- PO4 – Määratleda IT protsessid, organisatsioon ja seosed
- PO5 – Hallata IT-investeeringuid
- PO6 – Teavitada juhtimissihid ja suund
- PO7 – Hallata IT inimressursse
- PO11 – Hallata kvaliteeti (COBIT v3)
- TT3 – Hallata suutlikkust ja võimsust
- TT7 – Koolitada kasutajaid
- TT13 – Hallata käitust

BPR auditi puhul kõige asjassepuutuvamad teabekriteeriumid on

- toimivus,
- tõhusus,
- vastavus,
- teabe usaldatavus.

G27 Mobiilne andmetöötlus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S1 "Audititalituse põhikiri" määrab: "Infosüsteemide auditi talituse või infosüsteemide auditi ülesande täitja eesmärk, kohustused, õigused ja vastutus peaksid olema auditi põhikirjas või töövõtukirjas selgelt dokumenteeritud."

1.1.2 Standard S4 "Kutsealane pädevus" määrab: "IS audiitor peaks olema kutsealaselt pädev, tal peaksid olema auditiülesande täitmiseks vajalikud oskused ja teadmised."

1.1.3 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.4 Standard S6 "Audititöö sooritamine" määrab: "IS auditi personalile tuleks rakendada järelevalve mõistliku kinnituse saamiseks sellele, et auditi eesmärgid saavutatakse ja kohaldatavaid kutsealaseid auditeerimisstandardeid järgitakse."

1.1.5 Protseduur P8 "Turvalisuse hindamine. Läbistustestimine ja nõrkuste analüüs" sisaldab spetsiifiliste kontrollide sooritamise detailseid samme.

1.2 Seos COBITiga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- sooituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jäämise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooituse indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

G27 Mobiilne andmetöötlus (jätkub)

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

1.3 Suunise vajadus

1.3.1 Mobiilne ja traadita andmetöötlus on nähtus, mis on ülemaailmses äritegevuses hakanud endale tõmbama suurt tähelepanu. Mobiilne ja traadita andmetöötlus tähendab traadita side tehnoloogiate kasutamist juurdepääsuks võrgupõhistele rakendustele ja andmetele väga mitmesuguste mobiilseadmete abil. Selle tehnoloogia üha laiem kasutamine ja Interneti sirvimist võimaldavate uute portatiivsete seadmete kiire levik laiendab organisatsioonide füüsilisi piire ning nõuab IS audiitorilt selle tehnoloogia tundmist sellega kaasnevate riskide tuvastamiseks.

1.3.2 See suunis annab juhiseid IS auditeerimise standardite S1, S4 ja S5 rakendamise kohta mobiilse andmetöötluse turbe läbivaatusel auditiülesande ühe osana või eraldi läbivaatusena. IS audiitor peaks arvestama seda suunist otsustamisel, kuidas saavutada vastavus neile standarditele, kasutama ta rakendamisel kutsealast otsustusvõimet ning olema valmis põhjendama kõiki lahknevusi.

2 MÄÄRATLUSED

2.1 Traadita andmetöötlus

2.1.1 Traadita andmetöötlus tähendab andmetöötlusseadmete võimet suhelda nii, et nad saavad moodustada kohtvõrgu ilma kaabelduse infrastruktuurita, ning hõlmab tehnoloogiaid, mis koonduvad ümber IEEE 802.11x ja muude traadita side standardite, ja mobiilseadmetes kasutatavaid raadiosagedusriba teenuseid.

2.2 Mobiilne andmetöötlus

2.2.1 Termin "mobiilne andmetöötlus" laiendab seda tähendust seadmetele, mis võimaldavad uusi rakenduste kiike ja laiendavad ettevõtte võrku sellisel viisil, mis ei oleks võimalik muude vahenditega. Ta hõlmab pihuarvuteid, mobiiltelefone, sülearvuteid ning muid mobiiltehnoloogiaid ja neil põhinevaid tehnoloogiaid.

2.3 Kasutamine

2.3.1 Kuna mobiilseadmed on andmetöötlus- ja talletusvõimelised seadmed, saab neid mitmel viisil kasutada rakenduste ja andmete talletuseks, töötluseks ja võtuks. Neid saab kasutada poolautonoomsete seadmetena, mis töötlevad andmeid sõltumatul

viisil ja ühenduvad perioodiliselt mingi kesksüsteemiga või võrguga, et vahetada andmeid või rakendusi teiste süsteemidega, kuid neid saab kasutada ka klientsõlmedena, mis reaalajas pöörduvad teises kaugsüsteemis talletatavate andmete poole ja/või värskendavad neid (nad võivad töötada võrdsõlmedena või kuuluda mingisse hierarhiasse).

2.4 Käsitlusviis

2.4.1 Mobiilseadmed on arvutid, mis lõppkokkuvõttes koosnevad tavalistest komponentidest, nagu seda on riistvara, operatsioonisüsteem, rakendused ja sidekanalid. Käesolev dokument katab neid spetsiifilisi teemasid, mis on seotud seadme mobiilse andmetöötluse otstarbel kasutamise auditi või läbivaatusega. See dokument ei käsitle olemuslikke riske, mis on seotud aparatuuriga ja keskkonna ülejäänud osaga. (Katmata riskialade hulka jäävad näiteks tulemüüri konfiguratsioon, viirused ja programmide hooldus.)

3 LÄHTETINGIMUSED

3.1 Käsitlusala

3.1.1 IS audiitoril tuleks selgelt sõnastada mobiilse andmetöötluse eelseisva auditi eesmärgid ja käsitlusala; harilikult dokumenteeritakse need töövõtukirjas.

4 PLAANIMINE

4.1 Teabe kogumine

4.1.1 IS audiitor peaks hankima turvapoliitika, mis reguleerib lubatavat mobiilseadmete kasutamist.

4.1.2 IS audiitor peaks hankima teavet mobiilseadmete kavatsetud kasutamise kohta, selgitades välja, kus neid kasutatakse äritehinguteks ja andmetöötluseks ja/või tööviljakuse tõstmiseks (näiteks Interneti sirvimine, elektronpost, kalender, aadressiraamat, tööde meelespea), ning kasutatavate riistvara ja tarkvara tehnoloogiate kohta. Kesksed automatiseeritud ja käsiprotsessid tuleks dokumenteerida.

4.1.3 IS audiitor peaks hankima piisavalt teavet üksuse sooritatud riskianalüüsi kohta, koos sündmuste toimumise tõenäosuse ja võimaliku toimega, et hinnata üksuse mobiilse andmetöötluse keskkonna mõju.

4.1.4 IS audiitor peaks hankima piisavalt teavet mobiilse andmetöötluse halduseks kasutatavate poliitikate ja protseduuride kohta, mis hõlmavad side, riistvara, rakendustarkvara, andmeturbe, süsteemitarkvara, turvatarkvara jms aspektide kasutuselevõttu, käitust ja hooldust. Katta tuleks näiteks sellised alad nagu seadmete konfiguratsioon, füüsilised meetmed, kinnitatud tarkvara ja instrumendid, rakenduste turve, võrguturve, ootamatuste käsitluse plaanid, varundus ja taaste.

G27 Mobiilne andmetöötlus (jätkub)

4.1.5 Andmete kogumiseks, analüüsiks ja tõlgendamiseks tuleks sobivalt kasutada inimeste küsitlusi, dokumentatsiooni (näiteks äriplaani ja protokollide dokumentatsiooni) analüüsi ja traadita infrastruktuuri testimist.

4.1.6 Kui kasutatakse kolmandaid organisatsioone IS või tegevusalaste funktsioonide väljasttellimiseks, peaks IS audiitor vaatama läbi leppe tingimused, hinnates lepetes nõutavate turvameetmete sobivust ning organisatsiooni õigust perioodiliselt läbi vaadata teenuse andmisega seotud kolmanda poole keskkonda.

4.1.7 IS audiitor peaks vaatama läbi ka eelmiste uuringute aruanded ja arvestama plaanimisprotsessis nende tulemusi.

4.2 Riskianalüüs

4.2.1 IS audiitor peaks arvestama mobiilseadmete kasutamisega seotud riske ning siduma neid nendes seadmetes talletatava ja nende kaudu saadava teabe ning neis töödeldavate tehingute elutähtsusega tegevusalaselt, õiguslikult ja regulatiivselt seisukohalt.

4.2.2 Mobiilseadmete portatiivsus, suutvus, ühendatavus ja odavus võimaldab neid kasutada rakenduste töötluseks, kusjuures suurenevad näiteks sellised riskid:

- kahjustamine, kaotamine või vargus (portatiivsuse tõttu);
- võrguvarade kahjustamine mobiilseadmelt viiruste, usside vms saatmisega;
- volitamatu juurdepääs andmetele nende allalaadimise teel üleorganisatsioonilistest seadmetest või võrkudest (ühendatavuse tõttu);
- andmete volitamatud muutmised või lisamised nende üleslaadimise teel üleorganisatsioonilistesse seadmetesse või võrkudesse;
- volitamata juurdepääs seadmes asuvatele andmetele (seetõttu, et seadme operatsioonisüsteem on lihtne ja sisaldab harilikult ainult väga algelisi turbefunktsioone).

4.2.3 Riskianalüüsi sooritamisel tuleks arvestada järgmisi aspekte.

- Privaatsus: tähtis komponent tundliku teabe (näiteks krediitkaardinumbrite, rahaliste üksikasjade, haiguslugude) edastamisel. Privaatsusprotokollid ja nendega seotud protseduurid on väga tähtsad, sest traadita edastusi ei saa häkkerite juurdepääsu eest kaitsta muude vahenditega (näiteks füüsilise pääsu reguleerimise meetmetega).
- Autentimine: on võimalik tagada pääsmiku või sertifikaadiga , mida saab verifitseerida tunnustatud sertifitseerimisorgani (CA) abil.
- Kaksikautentimine: kasutatakse lõppkasutaja identiteedi ja seadme autentimiseks turvalise edastuse käigus (st saadakse kinnitus sellele, et nii seade kui ka kasutaja on volitatud agendid). Kaksikautentimist kasutatakse võrkupääsu keelamiseks seadmetelt, mis on kaotatud või varastatud.
- Andmeterviklus: sõnumi salvestamisel mobiilseadmesse tuvastatakse kõik edastamisel asetleidnud sõnumi sisu muutused.

- Salgamise vääramine: süsteem, mis takistab kasutajail eitamast, et nad on töödelnud mingi tehingu. Salgamise vääramine nõuab kasutaja edukat autentimist ning loob tehingu algataja kohta usaldatava ja õiguslikult siduva kirje.
- Konfidentsiaalsus ja krüpteerimine: sisaldab andmete sellist algoritmide abil teisendamist, mis takistab volitamata kasutajail või seadmeil nende andmete lugemist ja mõistmist (vt IS auditeerimise protseduur P9 "Krüpteerimis-metoodikate halduse meetmete hindamine"). Krüpteerimistehnoloogia põhineb võtmetel, millega krüpteeritakse ja dekrüpteeritakse andmeid nende edastamisel. Arvestada tuleks ka võtmete jaotamise ja turvalise hoidmise protseduure.
- Seadmete ja side volitamata kasutamine, sealhulgas risk sellest, et volitamata pääsu Internetti kasutatakse sissemurdmiseks kolmandate poolte võrkudesse (millest võib tuleneda kohtumenetlus organisatsiooni vastu).

4.2.4 IS audiitor peaks hindama tuvastatud ohtude materialiseerumise tõenäosust ja nende tõenäolist toimet ning dokumenteerima riskid koos meetmetega nende leevendamiseks. Sõltuvalt läbivaatuse käsitlusalast peaks IS audiitor võtma arvesse kõige tõenäolisemad ohuallikad, nii sisemised kui ka välised, näiteks häkkerid, konkurendid, ja välisriikide valitsused.

4.3 IS auditi eesmärgid

4.3.1 Vastavalt auditi eesmärkidele ja käsitlusalale peaks IS audiitor võtma läbivaatusele sellised turbealad nagu seda on

- side (kattes näiteks andmepüügi ja teenusetõkestuse riskid ning krüpteerimistehnoloogiate ja tõrketaluvuse protokollid);
- võrgu arhitektuur;
- virtuaalsed privaatvõrgud;
- rakenduste tarnimine;
- turvateadlikkus;
- kasutajate haldus;
- kasutaja- ja seansihaldus (kattes näiteks ülevõtu, spuufimise ja andmetervikluse kao riskid);
- füüsiline turve;
- avaliku võtme infrastruktuur;
- varunduse ja taaste protseduurid;
- käitus (näiteks reageerimine intsidentidele ja sisetöötlus);
- tehnoloogia arhitektuur (näiteks: sobiv, laiendatav kohandamiseks tegevusalaste vajadustega, kasutuskõlblik);
- turbe arhitektuur;

- turbetarkvara (näiteks sissetungi tuvastuse süsteem, tulemüür, viirusetõrje);
- turbe haldus;
- paikade rakendamine;
- jätkusuutlikkuse plaanimine.

4.4 Tööplaan

4.4.1 Saadud teabe põhjal ning ülesande käsitlusala ja eesmärkide põhjal peaks IS audiitor dokumenteerima selle, kuidas mõjutavad tuvastatud riskid ja nende riskide leevendamise meetmed tegevusalaseid, turbealaseid ja IS eesmärke (kui need on kohaldatavad).

4.4.2 Selle protsessi käigus peaks IS audiitor hindama nõrku kohti, mis vajavad tugevdamist. Kontrollimiseks tuleks tööplaani võtta uued turvameetmed, mis teadaolevalt leevendavad arvessevõetud riske.

5 AUDITITÖÖ SOORITAMINE

5.1 Sooritamine

5.1.1 Turvameetmete puudumisel peaks IS audiitor mõtlema plaanitud protseduuride laiendamisele (näiteks läbistustesti lisamisele) keskkonna tõeliste nõrkuste tuvastamiseks ning kontrollimiseks, kas need ei ole mõjutanud auditi eesmärke.

5.2 Aruandlus

5.2.1 Auditítöö lõpetamisel peaks IS audiitor esitama ettemääratud teenusekasutajaist adressaatidele sobivas vormis aruande.

5.2.2 IS audiitor peaks kaaluma aruande läbiarutamist asjakohaste huvipooltega enne aruande esitamist.

5.2.3 Aruanne peaks spetsifitseerima kõik ta levitamise kitsendused, mida IS audiitor või juhtkond on nõustunud rakendama. IS audiitor peaks kaaluma ka sellise lausungi lisamist, mis välistaks kohustused kolmandate suhtes.

6 JÕUSTUMISKUUPÄEV

6.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. septembril 2004 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

G27 Mobiilne andmetöötlus (jätkub)

LISA

Viited COBITile

Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ja arvestades COBITi teabekriteeriume.

Esmajärjekorras:

- PO9 – Hinnata IT riskid ja hallata neid
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE4 – Võimaldada käitus ja kasutamine
- HE5 – Hankida IT-ressursid
- HE6 – Hallata muutusi
- TT5 – Tagada süsteemide turvalisus
- TT9 – Hallata konfiguratsiooni
- SH2 – Seirata ja hinnata sisejuhtimist

Teises järjekorras:

- HE2 – Hankida rakendustarkvara ja hooldada seda
- TT8 – Hallata konsultatsioonipunkti ja intsidente

COBITi teabekriteeriumid on konfidentsiaalsus, terviklus ja käideldavus, tõhusus ja usaldatavus.

G28 Arvutikriminalistika

1 TAUST

1.1 Seos ISACA standarditega

1.1.1 Standard S3 "Kutse-eetika ja standardid" määrab: "IS audiitor peaks auditiülesannete täitmisel järgima ISACA kutse-eetika koodeksit."

1.1.2 Standard S3 "Kutse-eetika ja standardid" määrab: "Auditiülesannete täitmisel peaks IS audiitor ilmutama vajalikku kutsealast hoolikust, sealhulgas järgima kohaldatavaid kutsealaseid auditeerimise standardeid."

1.1.3 Standard S4 "Kutsealane pädevus" määrab: "IS audiitor peaks olema kutsealaselt pädev, tal peaksid olema auditiülesande täitmiseks vajalikud oskused ja teadmised."

1.1.4 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.5 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.2 Seos COBITiga

1.2.1 1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- soorituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jäämise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusse indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside, juhtimiseesmärkide, nendega seotud juhtimistavade valimisel ja asjassepuutuvate COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

1.3 Suunise vajadus

1.3.1 IS audiitorilt küsitakse sageli nõu arvuti- või sidesüsteemidega sooritatud pettuste või korratuste (arvutikelmuste) kohta ning soovitakse, et ta kontrolliks organisatsiooni vastavust arvutialastele seadustele või eeskirjadele. Et aidata organisatsioonil leida või vältida selliseid korratusi, on vaja algteadmisi arvutikriminalistikast. See dokument on mõeldud aitama IS audiitoril saavutada seda eesmärki.

1.3.2 Arvutikriminalistika esmane eesmärk on andmete viivitamatu tabamise teel selgitada välja mingis konkreetses olukorras peituv tõde, et tuvastada ründaja ja õiguskaitse abistamiseks leida tõendus kriminaalmenetluse tarbeks. Ta aitab ka organisatsioonil kaitsta infovarasid tulevaste rünnete eest ning õppida tundma ründajaid ja ründeid. Peamised tunnusomadused on

- rõhk vajadusel viivitamatult reageerida, nii et asitõendid ei läheks kaotsi ja neid ei manipuleeritaks;
- rikkumiskohale võimalikult lähedaste andmete hõive ja säilitamine;
- asitõendite ekspertiisikõlblik säilitamine võimalikuks esitamiseks kohtus;
- minimaalselt sekkuv andmehõiveprotsess, talitluse katkestamiseta;
- ründaja tuvastamine ja tõenduse leidmine.

1.3.3 Arvutijuurdluse läbiviimise ajal on väga oluline säilitada kogutud andmete ja teabe konfidentsiaalsus ja terviklus ning teha need andmed kättesaadavaiks ainult asjakohastele ametiisikutele. Sellistel juhtudel on IS audiitoril oluline roll ning ta võib abistada organisatsiooni sellega, et ütleb, kas tuleks konsulteerida juristiga ning milliseid IS keskkonna tehnilisi aspekte tuleks asjakohaselt uurida. Mõnedel juhtudel võidakse IS audiitorile anda teavet kahtlustatava korratuse või ebaseadusliku toimingu kohta ning soovida, et ta kasutaks lisateabe kogumiseks andmete analüüsi võimalusi.

1.3.4 Arvutikriminalistikat on rakendatud paljudel aladel, sealhulgas pettuse, spionaaži, mõrvade, väljapressimise, arvuti väärkasutuse, tehnoloogia kuritarvituse, laimu, ähvarduskirjade, infolekete, intellektuaalse omandi varguse, pornograafia, rämpsposti, häkkimise ja ebaseaduslike rahaülekannete uurimiseks.

G28 Arvutikriminalistika (jätkub)

Arvutikriminalistika sisaldab sündmuste detailset analüüsi küberruumis ja asitõendite kogumist. See suunis kirjeldab lühidalt arvutikriminalistika elemente, eesmärgiga aidata IS audiitoril arvestada selliseid aspekte, kui seda nõuab mingi olukord ülesande täitmise käigus. IS audiitor peaks arvutikriminalistika vajadusest teatama ka sisejuurdluse tarbeks, sest väliste rünnetega võrreldes moodustavad suure protsendi kriminalistikauuringutest

- kaebused sisemistelt informeerijailt;
- personaliosakonna juurdlused;
- pettuse juurdlused;
- vastavuse uuringud: nõuavad vastavust mitmesugustele õigusaktidele ja tegevusala suunistele (näiteks: Sarbanes-Oxley, NIST, FISMA).

1.3.5 See suunis annab juhiseid IS auditeerimise standardite S3 "Kutse-eetika ja standardid", S4 "Kutsealane pädevus", S5 "Plaanimine", S6 "Audititöö sooritamine" rakendamiseks arvutikriminalistliku läbivaatuse sooritamisel. IS audiitor peaks arvestama seda suunist, kui ta otsustab, kuidas saavutada vastavus ülalnimetatud standarditele, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama kõiki lahknevusi.

1.4 Suunise rakendamine

1.4.1 Selle suunise rakendamisel peaks IS audiitor arvestama selle juhiseid kooskõlas muude asjassepuutuvate ISACA suunistega.

1.4.2 Arvutikriminalistliku ülesande täitmisel peaks IS audiitor vajaduse korral tutvuma vastavas jurisdiktsioonis kehtivate kohtuliku juurdluse juhistega.

2 MÄÄRATLUSED

2.1 Arvutikriminalistika

2.1.1 Arvutikriminalistikat võib määratleda kui protsessi, millega arvuti salvestuskandjalt eraldatakse välja teavet ja andmeid juriidiliselt kõlblike vahendite ja tehnoloogiaga ning äraproovitult parimate kriminalistikatavadega nende andmete täpsuse ja usaldatavuse saavutamiseks, eesmärgiga esitada neid andmeid asitõendina.

2.1.2 Arvutikriminalistika ees olev jõuproov seisneb tegelikult nende andmete leidmises, kogumises, säilitamises ja esitamises loetaval kujul, mis on aktsepteeritav kohtus.

2.1.3 Arvutikriminalistika sisaldab eelkõige teaduslikult tõestatud meetodite uurimist ja rakendamist digitaalsete asitõendite kogumiseks, tõlgendamiseks ja kasutamiseks mingi väite toetuseks, näiteks, et

- sooritada kõigi toimingute otsustav juurdlus eesmärgiga kontrollida rünnet täielikult ning taastada ettevõtte ja elutähtsa infrastruktuuri teave;

- korreleerida, tõlgendada ja prognoosida kahjulikke toiminguid ja nende mõju plaanilisele tegevusele;
- teha digitaalandmed sobivaiks ja veenvaiks nende rakendamiseks kohtuliku juurdluse protsessis.

2.1.4 Arvutikriminalistika on nii teadus kui ka kunst arvutist andmete väljaeraldamiseks ja kogumiseks eesmärgiga otsustada, kas ja kuidas on toimunud kuritarvitus või sissetung, millal see toimus ja kes oli sissetungija. Raskusteta on võimelised neid eesmärke saavutama organisatsioonid, kes rakendavad häid turbetavasid ja peavad asjakohaseid logisid. Õigete teadmiste ja vahenditega saab aga kohtulikke asitõendeid välja eraldada isegi põlenud, vees ligunenud või füüsiliselt kahjustatud arvutisüsteemidest.

3 AUDITI PÕHIKIRI

3.1 Ülesandemandaat

3.1.1 Enne arvutikriminalistikaga seotud ülesande täitmisele asumist peaks IS audiitor taotlema vastavalt ametiisikult ülesande täitmiseks selge kirjaliku mandaadi.

3.1.2 Mandaat peaks spetsifitseerima ülesande kohustused, õigused ja kitsendused ning tagama IS audiitori sõltumatuse selle ülesande täitmisel. Ta peaks ka tegema selgeks, et audiitor tegutseb seadusliku õigusega, mis annab talle juurdepääsu asjassepuutuvatele süsteemidele ja andmetele.

3.1.3 Kui IS audiitor kasutab ülesande täitmiseks välist asjatundjat, peaks mandaat spetsifitseerima ka käsitlusala ja kohustused.

4 SÕLTUMATUS

4.1 Sõltumatuse kaalutlusi

4.1.1 Enne arvutikriminalistikaga seotud ülesande täitmisele asumist peaks IS audiitor andma mõistliku kinnituse sellele, et puudub igasugune huvide vastuolu.

4.1.2 Kui arvutikriminalistliku ülesande algatas valitsus, riigiasutus või ametiisik, peaks IS audiitor selgelt teatama oma sõltumatusest ja õigusest täita seda ülesannet, säilitama hangitud teabe konfidentsiaalsuse, olema erapooletu ja esitama aruanded asjakohastele ametivõimudele.

G28 Arvutikriminalistika (jätkub)

5 AUDITI KAALUTLUSI

5.1 Elektroonilise tehingu juriidiline kehtivus

5.1.1 Et kaupade või teenuste müüki sisaldav lepingut saaks lugeda kehtivaks, peaks ta olema alla kirjutatud. Elektrooniliste lepingute puhul saab seda teha digitaalallkirjaga.

5.1.2 Digitaalallkiri võib saavutada juriidilise kehtivuse eesmärgi järgmiselt.

- Autentimine: on olemas tõend andmete päritolu kohta.
- Terviklus: verifitseerimisprotsess õnnestub ainult siis, kui sõnum ei ole muutunud.
- Salgamise vääramine ehk autorlus: igal võtme kasutajal on juriidiline kohustus kaitsta oma võtit. Seetõttu ta ei saa lahti öelda allakirjutatud dokumendi sisust ega seda ühepoolselt muuta. Privaatvõtme kaitseks kasutatav kõlblik süsteem võib võtit talletada mingis turvalises personaalses seadises, näiteks kiipkaardis. Kas omaenda digitaalallkirja on võimalik eitada? Isegi kui seda peetaks lubatavaks, poleks eitamisest kasu. Teisel osapoolel tuleks ainult tõestada, et lepingu allakirjutamisel allkiri kehtis. See tähendab, et võtme omanik peaks tõestama, et tema privaatvõti varastati või allutati volitamata kasutusele enne lepingu allakirjutamise hetke. Digitaalallkirja ei saa eitada, kui selle on autentinud notar.
- Konfidentsiaalsus: allakirjutatud dokumendile konfidentsiaalsuse lisamiseks tuleb dokument lihtsalt krüpteerida adressaadi avaliku võtmega.

5.2 Osapoolte ja tehingu sisu piiritlemine

5.2.1 Lepingut sõlmima on pädevad ainult täisealised (enamikus jurisdiktsioonides 18-aastased või vanemad).

5.2.2 Kauplejad võivad kasutada kõiki vahendeid endale tõendamiseks, et teisel poolel on juriidiline õigus tehingut sooritada. Nad võivad taotleda igasugust tõestust ja jätkata ostja andmete talletust oma arhiivides. Vea või kuritarvituse korral vastutab lepingu õige täitmise eest lõppkokkuvõttes kaupleja. Digitaalallkirja süsteemi kasutamisel on vastutus organil, kes andis välja digitaalallkirja. Seda organit nimetatakse sertifitseerimiskeskuseks (CA). Vaidlustamise puhul peaks digitaalsertifikaadi omanik tõendama, et ta privaatvõti varastati või seda kuritarvitati.

5.2.3 Samad asjaolud kehtivad tehingu sisu (tervikluse) puhul: see säilib digitaalallkirja süsteemi kasutamisel. Vastasel juhul vastutab kaupleja väärade, puudulike, mitmetähenduslike ja vigaste andmete eest.

5.2.4 Krediitkaardipettuste ja privaatsuse rikkumise eest vastutab alati kaupleja.

5.3 Lepingu sõlmimise koht

5.3.1 Elektronkaubanduse puhul on suurim probleem lepingu sõlmimise täpse asukoha määramine; see määrab jurisdiktsiooni ja kohaldatavad õigusaktid.

5.3.2 Lepingule kohaldatava spetsiifilise seaduse puudumisel on ainsaks alternatiiviks toetumine rahvusvahelisele jurisdiktsioonile. Nüüdistehnoloogia võimaldab igaühel saada kõikjal kogu maailmas saada ühendust oma teenuseandjaga. Seetõttu on võimatu määratleda täpset asukohta, kus leping sõlmitakse.

5.3.3 Lahendus on rahvusvahelise õiguse õige rakendamine ja sellest tulenev rahvusvaheliste lepete rakendamine. [2]

5.3.4 Tunnustatuim lähenemisviis määrab, et

- kui pooled on valinud mingi konkreetse seadustiku, on see ainus kohaldatav seadustik;
- kui pooled ei ole valinud mingit seadustikku, kohaldatakse seadustikku, mis on lähemalt seotud lepinguga (näiteks teenuseandja asukohamaa oma), või, toote müümisel tarbija maa oma.

5.3.5 Igal juhul on vältimatu kõikvõimalik ettevaatus, sest müüja asukohta on äärmiselt raske kindlaks teha (ja tõestada).

5.4 Kategooriate eristamine

5.4.1 Sõltumata lepingu sõlmimise asjaoludest on teabekäsitlusele loomuomane liigitada hankija tarbijaks, sest kõigis maades kaitsevad õigusaktid tarbijat. Seetõttu eristatakse ettevõtetevahelist ning ettevõtte ja tarbija vahelist elektroonilist kaubandust.

5.5 Pettuse vältimine

5.5.1 Majandussüsteem on rajatud ühelt poolt pakkumuste või nõustumiste identifitseerimisele ja salgamise vääramisele, teiselt poolt selliste arvelduste loomisele, mis on mõistlikult turvalised nii sel juhul, kui isik ostab (mis tähendab, et ta soovib saada teenuseid või kaupu), kui ka juhul, kui see isik müüb (mis tähendab, et ta soovib saada makseid). Tänapäeval näib digitaalallkirjaga süsteem olevat ainus seadusjärgne võrgu kaudu maksmise vorm.

[2] Rooma konventsioon, 1980, Euroopa õigusakt, *www.rome-convention.org/instruments/i_conv_cons_it.htm* ja Viini konventsioon, 1980. a. allakirjutatud rahvusvaheline lepe kaupade impordi ja ekspordi kohta, *www.cisg.law.pace.edu/cisg/biblio/volken.html*.

G28 Arvutikriminalistika (jätkub)

5.6 Krediitkaartide kasutamine Interneti kaudu

5.6.1 Krediitkaart on praegu kõige kasutatavam Interneti kaudu tehtavate tehingute makseinstrument. Kahjuks on olemas palju võimalusi krediitkaardi andmete kuritarvituseks (näiteks võimalus reprodutseerida neid andmeid võrgus). Näiteks on võimalik, et tehingu kviteerimist võib lugeda keegi, kes pole selleks volitatud.

5.6.2 Võrgutehingute tegemiseks pole krediitkaart ise vajalik, piisab ta andmetest. Krediitkaardikelmused sooritatakse lihtsalt kaardi andmeid volitamatult kasutades. Krediitkaardikelmusi on kolme liiki:

- kaardi andmete kuritarvitamine;
- krediitkaardi võltsimine ja võltskaardi omamine;
- ebaseadusliku kaardi müümine või ostmine.

5.6.3 Krediitkaardi ebaseaduslik kasutamine Interneti kaudu tähendab igasugust toimingut, mis kaardi andmeid kasutades üritab pettusega saada raha, kaupu või teenuseid. Kuritegu on ka see, kui kaardi omanik kasutab aegunud kaarti.

6 ARVUTIKRIMINALISTIKA KESKSED ELEMENDID AUDITI PLAANIMISEKS

6.1 Andmete kaitse

6.1.1 Väga oluline on rakendada meetmeid, millega vältida otsitava teabe hävimine, rikkumine ja kättesaamatuks muutumine.

6.1.2 Tähtis on ka teavitada asjakohaseid pooli sellest, et elektroonilisi asitõendeid hakatakse otsima nende avastamise teel arvutisüsteemides, rakendades spetsiifilisi protokolle, mis nõuavad, et kõik pooled säilitaksid elektroonilised asitõendid ega püüaks igasuguste vahenditega hävitada teavet.

6.1.3 Reageerimisvõime ja kriminalistliku juurdluse võime tuleks luua enne intsidendi või sündmuse toimumist. See hõlmab infrastruktuuri ja protsesse intsidentidele reageerimiseks ja nende käsitluseks.

6.2 Andmehõive

6.2.1 Kujutab endast protsessi teabe ja andmete üleviimiseks mingisse ohjatavasse kohta.

6.2.2 Sisaldab igat liiki elektrooniliste andmekandjate, näiteks kettadraivide, lindidraivide, diskettide, varunduslintide, zip-salvestite ja igasuguste muude ird-andmekandjate kogumist. Kõik andmekandjad tuleb kaitsta, viies mingi aktsepteeritava meetodiga nende sisu (kujutise) üle teisele andmekandjale. Peale selle on tähtis kontrollida, kas andmekandjatel ei ole viiruseid ja kas nad on kaitstud kirjutuse eest.

6.2.3 Andmeid ja teavet hõivatakse ka tunnistajate ja teiste asjaosaliste ütluste salvestamise teel.

6.2.4 Paljudel juhtudel on väga oluline püüda kinni ajutised andmed, sealhulgas avatud pordid, avatud failid, aktiivsed protsessid, kasutajate sisselogimised aj muud andmed põhimälus. Ajutised andmed on lühiealised ja lähevad arvuti sulgemisel kaotsi. Ajutiste andmete püük aitab uurijail otsustada, mis süsteemis hetkel toimub.

6.3 Bittkujutised

6.3.1 Bittkujutiste loomine tähendab hõivatud andmete bitthaaval kopeerimist sellise kustutamatu faksiimilejäljendi saamiseks, millele saab rakendada paljusid analüüse, ilma et oleks karta esialgsete andmete või teabe kahjustamist.

6.3.2 Bittkujutisi luuakse uuritava salvesti jääkandmete püügiks. Bittkujutis kopeerib ketta pinna sektorhaaval, mitte failhaaval koopiana, mis ei jäädvusta jääkandmeid. Jääkandmete hulka kuuluvad kustutatud failid, kustutatud failide fragmendid ja muud andmed, mis on ketta pinnal endiselt olemas. Sobivate vahenditega saab ketta pinnalt taastada ka hävinud andmeid (kustutatud andmeid, isegi salvestuskandja ümbervormindusega kustutatuid).

6.4 Ekstraktimine

6.4.1 See tähendab potentsiaalselt kasulike andmete tuvastust andmekogumi bittkujutises ja nende eraldamist. See hõlmab kahjustatud, rikutud või hävinud andmete taastamist ja avastamise vältimiseks manipuleeritud andmete taastamist.

6.4.2 Kogu kujutiseloome ja ekstraktimise protsess peab vastama kvaliteedi, tervikluse ja usaldatavuse normidele. See puudutab ka kujutise loomiseks kasutatavat tarkvara ja andmekandjat, millel kujutis luuakse. Üks hea näitaja oleks: kas seda tarkvara on kasutanud, sellele toetunud või seda kinnitanud õiguskaitseasutused. Koopiaid ja asitõendeid peab olema võimalik verifitseerida sõltumatult, st oponenti ja kohut peab saama veenda, et andmed on õiged, usaldusväärsed ja manipuleerimiskindlad.

6.4.3 Ekstraktimisel uuritakse paljusid andmeallikaid, näiteks süsteemilogisid, tulemüüri logisid, sissetungi tuvastuse süsteemi logisid, kontrolljälgi ja võrguhalduse teavet.

6.5 Andmeusutlus

6.5.1 See tähendab päringuid ekstraktitud andmetes eesmärgiga välja selgitada, kas neis andmetes on olulisi seoste näitajaid, näiteks telefoninumbreid, IP-aadresse ja isikute nimesid.

6.5.2 Ekstraktitud andmete korralik analüüs on oluline soovituste tegemiseks ja õiguskaitseorganitele asitõendite esitamiseks sobiva pinna ettevalmistamiseks.

G28 Arvutikriminalistika (jätkub)

6.6 Andmete valmendus ja normaliseerimine

6.6.1 See tähendab ekstraktitud andmete üleviimist ja talletust sobivate meetoditega ja uurijaile raskusteta arusaadavas vormingus. Võib sisaldada kuueteistkümnend- või kahendandmete teisendamist loetavateks märkideks, andmete teisendamist mingi teise keele ASCII-märgistikku või teisendamist mingisse andmeanalüüsi vahendite jaoks sobivasse vormingusse.

6.6.2 Juurdlushüpoteeside püstitamiseks ekstrapoleeritakse võimalikke seoseid andmetes sulandamise, korreleerimise, diagrammimise, vastendamise, ajalise järjestamise jt meetoditega.

7 ARUANDLUS

7.1 Juriidiline aktsepteeritavus

7.1.1 Nagu juba öeldud, on arvutikriminalistika ees seisev jõuproov andmete leidmine, kogumine säilitamine ja esitamine nii, et seda aktsepteeriks kohus. IS audiitoril peaks olema täielik teave ja selgus aruande ettemääratud adressaatide ja eesmärgi kohta.

7.1.2 Aruandel peaks olema sobiv vorm ning ta peaks sõnastama sooritatud uuringu käsitlusala, eesmärgid, iseloomu, ajastuse ja ulatuse.

7.1.3 Aruandesse tuleks märkida organisatsioon, määratud adressaadid ja levitamise kitsendused (kui neid on). Aruanne peaks selgelt teatama leiud, järeldused ja soovitused, koos IS audiitori kõigi reservatsioonidega ülesande suhtes.

7.2 Asitõendid

7.2.1 Elektrooniliste asitõendite valik ulatub suurarvutitest ja pihuarvutitest diskettide, CD-de lintide ja isegi vähimate kiipideni.

7.2.2 Mõistliku tagatise saamiseks sellele, et asitõendeid ei manipuleerita ega hävitata, tuleks järgida valdkonnas spetsifitseeritud parimaid tavasid, kasutada äraproovitud vahendeid ja ilmutada asjakohast hoolikust. Terviklus, usaldatavus ja konfidentsiaalsus on absoluutselt vajalikud, et õiguskaitseorganid jõuaksid õiglase otsuseni. Väga tähtis on ka see, et asitõendid hangitaks ja esitataks ametivõimudele õigel ajal.

7.2.3 Interneti meili jälituse näide.

- Interneti meilisõnumi saatmisel täidab kasutaja tavaliselt ainult saaja(te) rea(d) (*To* ja *Cc*) ja teemarea.

G28 Arvutikriminalistika (jätkub)

- Sõnumi töötlemisel lisab meilitarkvara ülejäänud osa päiseteabest. Järgnevas on meilipäise näide.

```
----- Message header follows -----
(1)  Return-path: <sasrock@o199632.cc.nps.gov.org>
(2)  Received: from o199632.cc.navy.gov by nps.gov.org (5.1/SMI-5.1) id AAO979O;
     Fri, 7 Nov 2003 18:51:49 PST
(3)  Received: from localhost byo199632.gov.org (5.1/SMI-5.1) id AA41651; Fri 7
     Nov 2003 18:50:53 PST
(4)  Message-ID: <9611080150.AA16514@o199632.cc.navy.gov>
(5)  Date: Fri, 7 Nov 2003 18:50:53 -0800 (PST)
(6)  From: "Susan Rock" <sasrock@o199632.cc.nps.gov.org>
(7)  To: Mott Thick <mott.thick@ocean.com>
(8)  Cc: Jokey Ram<J.ram@seabeas.com>
```

- Rida (1) ütleb saaja-arvutitele, kes saatis selle sõnumi ja kuhu saata veateated (tagastused ja hoiatused).
- Read (2) ja (3) näitavad sõnumi marsruuti saatmisest saabumiseni. Iga arvuti, mis saab selle sõnumi, lisab oma täieliku aadressiga ja ajatempliga saamisvälja (*Received*:); see aitab jälitada kohaletoimetuse probleeme.
- Rida (4) on sõnumi identifikaator, selle konkreetse sõnumi ühene identifikaator. See identifikaator logitakse ja seda saab jälitada läbi kõigi arvutite selle sõnumi marsruudil, kui on vaja jälitada meili.
- Rida (5) näitab sõnumi saatmise kuupäeva, kellaaega ja ajavööndit.
- Rida (6) näitab sõnumi algataja (saatja) nime ja meiliaadressi.
- Rida (7) näitab esmase saaja nime ja meiliaadressi; see aadress võib kuuluda

  - meililistile,

  - pseudonüümile kogu süsteemi ulatuses,

  - personaalsele kasutajanimele.

- Rida (8) loetleb sõnumi koopia (*Cc*) saajate nimed ja meiliaadressid. Võimalikud on ka salakoopiad (Bcc); nende saajad saavad sõnumi koopia, kuid nende nimesid ja aadresse ei ole päistes näha.

8 JÕUSTUMISKUUPÄEV

8.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. septembril 2004 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

G28 Arvutikriminalistika (jätkub)

LISA

Viited COBITile

Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi protsesside valimise põhjal ning arvestades COBITi juhtimiseesmärke ja nendega seotud haldustavasid. Arvutikriminalistliku läbivaatuse tarbeks tõenäoliselt kõige asjakohasemad COBITi protsessid on alljärgnevas liigitatud esmasteks ja teisesteks. Protsessid ja juhtimiseesmärgid, mis tuleb valida ja rakendada, võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest.

Esmajärjekorras:

- PO8 – Tagada vastavus välisnõuetele (COBIT v3)
- HE1 – Tuvastada automatiseeritud lahendused
- TT1 – Määratleda teenusetasemed ja hallata neid
- TT2 – Hallata kolmandate osapoolte teenuseid
- TT5 – Tagada süsteemide turvalisus
- TT10 – Hallata probleeme
- TT11 – Hallata andmeid
- SH1 – Seirata ja hinnata IT töötulemusi
- S3 – Saada sõltumatu kinnitus (COBIT v3)

Teises järjekorras:

- PO1 – Määratleda strateegiline IT plaan
- PO4 – Määratleda IT protsessid, organisatsioon ja seosed
- TT6 – Tuvastada ja kinnistada kulud
- TT12 – Hallata füüsilist keskkonda
- TT13 – Hallata käitust
- SH2 – Seirata ja hinnata sisejuhtimist

Arvutikriminalistliku läbivaatuse jaoks kõige asjakohasemad COBITi teabekriteeriumid on

- esmajärjekorras: usaldatavus, terviklus ja vastavus;
- teises järjekorras: konfidentsiaalsus ja käideldavus.

G29 Teostusjärgne läbivaatus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.2 Standard S8 "Järeltoimingud" määrab: "Pärast leidude ja soovituste teatamist aruandes peaks IS audiitor taotlema asjakohast teavet ja hindama seda otsustamiseks, kas juhtkond on õigel ajal rakendanud asjakohaseid meetmeid."

1.2 Seos COBITiga

1.2.1 Lai juhtimiseesmärk S4 "Korraldada sõltumatu audit" (COBIT v3) määrab: "Sõltumatu auditi korraldamise IT-protsessi juhtimist, mis rahuldab ärinõuet tõsta usaldustasemeid ja saada kasu parimal taval põhinevatest nõuannetest, võimaldavad sõltumatud korrapäraste vaheaegade järel sooritatavad auditid, kusjuures võetakse arvesse

- auditi sõltumatus,
- ettenägelik osalemine auditis,
- auditi sooritamine kvalifitseeritud personaliga,
- kokkuleppimine leidude ja soovituste suhtes,
- järeltoimingud,
- auditi soovituste toime hinnangud (kulud, tulud, riskid).

1.2.2 Detailne juhtimiseesmärk S4.6 "Audititöö sooritamine" (COBIT v3) määrab: "Auditite tuleks asjakohaselt rakendada järelevalve kinnituse saamiseks sellele, et auditi eesmärgid saavutatakse ja kohaldatavaid kutsealaseid auditeerimisstandardeid järgitakse.

Audiitorid peaksid tagama, et nad hangivad toimivaks auditi eesmärkide saavutamiseks piisavad, usaldusväärsed, asjassepuutuvad ja kasulikud asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite sobiva analüüsi ja tõlgendamisega

1.3 Toetumine COBITile

1.3.1 Toetumine COBITile pakub spetsiifilisi COBITi eesmärke või protsesse, mida tuleks arvestada selles suunises käsitletava ala läbivaatusel. Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ja arvestades COBITi teabekriteeriume.

G29 Teostusjärgne läbivaatus (jätkub)

1.3.2 Teostusjärgses läbivaatuses, mis on esimene läbivaatus pärast IT-lahenduse teostamist, on asjakohasemad alljärgnevad protsessid.

- PO2 – Määratleda infoarhitektuur
- PO4 – Määratleda IT protsessid, organisatsioon ja seosed
- PO5 – Hallata IT-investeeringuid
- PO8 – Tagada vastavus välisnõuetele (COBIT v3)
- PO9 – Hinnata IT riskid ja hallata neid
- PO10 – Hallata projekte
- PO11 – Hallata kvaliteeti (COBIT v3)
- HE1 – Tuvastada automatiseeritud lahendused
- HE2 – Hankida rakendustarkvara ja hooldada seda
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE5 – Hankida IT-ressursid
- HE6 – Hallata muutusi
- TT7 – Koolitada kasutajaid
- TT11 – Hallata andmeid
- SH1 – Seirata ja hinnata IT töötulemusi

1.3.3 Teostusjärgse läbivaatuse puhul kõige asjassepuutuvamad teabekriteeriumid on

- eelkõige toimivus ja tõhusus;
- seejärel käideldavus, vastavus, konfidentsiaalsus, usaldatavus ja terviklus.

1.3.4 Rahvusvahelise Raamatupidajate Föderatsiooni (IFAC) infotehnoloogiakomisjoni (ITC) suuniste hulka kuuluvad

- Infotehnoloogiliste lahenduste teostamine
- Äriliselt toimiva infotehnoloogia plaanimise haldus

1.4 Suunise eesmärk

1.4.1 Selle suunise eesmärk on kirjeldada soovitatavaid tavasid infotehnoloogiliste lahenduste teostusjärgse läbivaatuse sooritamiseks nii, et läbivaatuse kestel järgitaks asjassepuutuvaid infosüsteemide auditeerimise standardeid.

1.4.2 Organisatsioonid rakendavad oma ärivajaduste rahuldamiseks mitmesuguseid IT-lahendusi. Kui lahendused on juba teostatud, sooritavad IS audiitorid tavaliselt teostusjärgseid läbivaatusi, et hinnata IT-lahenduste ja nende teostuste toimivust ja tõhusust, algatada (vajaduse korral) toiminguid lahenduse täiustamiseks ja saada õppevahend edaspidise tarbeks.

G29 Teostusjärgne läbivaatus (jätkub)

1.4.3 Mõned selles suunises soovitatud tavad võivad sobida ka selliste projektide läbivaatusteks, mille teostus oli edutu või mis katkestati enne teostamist.

1.4.4 See suunis annab juhiseid IS auditeerimise standardite S6 "Auditi töö sooritamine" ja S8 "Järeltoimingud" rakendamiseks teostusjärgse läbivaatuse sooritamisel. IS audiitor peaks seda suunist arvestama otsustamisel, kuidas saavutada nende standardite rakendamine, kasutama suunise rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama kõiki lahknevusi.

1.5 Suunise rakendamine

1.5.1 Selle suunise rakendamisel peaks IS audiitor arvestama ta juhiseid seostatult muude asjassepuutuvate ISACA suunistega.

1.6 Määratlus ja üldine katvus

1.6.1 Käesoleva suunise otstarbeks tähendab teostusjärgne läbivaatus IT-lahenduse ja/või selle teostamise protsessi esimest või sellele järgnevat läbivaatust, mis sooritatakse pärast lahenduse teostamist eesmärgiga hinnata ükskõik milliseid aspekte alljärgnevate hulgast.

- Kas lahendusele seatud eesmärgid saavutati?
- Kas tegelikke kulusid ja tulusid on võrreldud eelarvega?
- Teostusprotsessi toimivus ja sobivus.
- Aja ja/või maksumuse ülekulude põhjused ning kvalteedi- ja või sooritusprobleemid, kui neid on.
- Tootlikkuse ja soorituse tõus lahenduse tulemusena.
- Kas äriprotsess ja sisemeetmed on teostatud?
- Kas kasutajate juurdepääsu reguleerimise meetmed on teostatud vastavalt organisatsiooni poliitikale?
- Kas kasutajaid on asjakohaselt koolitatud?
- Kas süsteem on hooldatav ja kas teda saab toimivalt ja tõhusalt edasi arendada?
- Kas asjassepuutuvad olemasolevad erijooned ja protseduurid on teostatud?
- Vastavus asjassepuutuvatele põhikirja nõuetele ja/või organisatsiooni poliitikatele.
- Vastavus asjassepuutuvatele COBITi juhtimiseesmärkidele ja/või COBITi juhtkonna suunistele.
- Lahenduse või teostusprotsessi edasise täiustamise võimalused.

1.6.2 Teostusjärgse läbivaatuse eesmärkide hulka võivad kuuluda järgmised.

- Veenduda, et IT-lahenduse teostamisele seatud eesmärgid saavutati ja et need on suunatud organisatsiooni ärieesmärkide saavutamisele.

G29 Teostusjärgne läbivaatus (jätkub)

- Hinnata sisestusele, töötlusele ja väljastusele rakendatud protseduuride ja meetmete adekvaatsust veendumiseks, et hõivatud teave on täielik ja täpne, infotöötlus vastab vajalikele talitlusreeglitele ning genereeritav teave on täpne, usaldatav ja õigeaegne.
- Hinnata IT-lahenduses tekitatavate kontrolljälgede hooldusele ja seirele rakendatavate protseduuride ja meetmete adekvaatsust.
- Kontrollida IT-lahenduses genereeritavate rahandus- ja haldusaruannete õigsust.
- Veenduda IT-lahenduses kehtestatud rakendustaseme meetmete adekvaatsuses.
- Kontrollida IT-lahendusele omaste käideldavusfunktsioonide adekvaatsust talitluse taastamiseks pärast iga ootamatut seisakut ja andmete tervikluse säilitamiseks.
- Veenduda, et IT-lahendust saab toimivalt ja tõhusalt toetada ja hooldada ka ta väljatöötamise ja teostamise eest vastutava eripersonali puudumisel.
- Tuvastada potentsiaalsed riskid ja meetmete nõrkused ning pakkuda lahendusi riskide leevendamiseks ja meetmete tugevdamiseks.

1.6.3 Sisuliselt püüab teostusjärgne läbivaatus teha kindlaks kas investeering IT-lahendusse õigustas end (organisatsiooni poolt määratud ja mõõdetavas väljenduses) ning kas loodud IT-lahendust saab adekvaatselt hallata ja juhtida. Niisugust investeeringu tasuvust võib katta ühe eraldi läbivaatusega, mida sageli nimetatakse kasu realiseerumise läbivaatuseks (jaotis 8.1). Teostusjärgse läbivaatuse käsitlusala peaks arvestama alljärgnevat.

- IT-lahenduse iseloom.
- IT-lahenduse kavatsetav kasutamine (milliseks otstarbeks, kes kasutab, millal ja kus).
- IT-lahenduse olulisus ärieesmärkide saavutamiseks.
- Auditeeritava üksuse (organisatsiooni) juhtkonnaga kokkulepitud läbivaatuse käsitlusala.
- Kas IT-lahenduse auditiläbivaatusi korraldati ta algatamise, väljatöötamise ja testimise järkudes?
- Kas projekti teostamise ajal on olnud IS audiitorite auditivälist osalemist?

2 AUDITI PÕHIKIRI

2.1 Volitused

2.1.1 Enne teostusjärgse läbivaatuse alustamist peaksid IS audiitoril olema läbivaatuse sooritamiseks asjakohased volitused. Kui läbivaatuse algatas kolmas pool, peaks IS audiitor saama mõistliku kinnituse sellele, et kolmandal poolel on asjakohane õigus korraldada läbivaatust.

G29 Teostusjärgne läbivaatus (jätkub)

3 SÕLTUMATUS

3.1 Kutsealane objektiivsus

3.1.1 Enne ülesande vastuvõtmist peaks IS audiitor andma mõistliku kinnituse sellele, et tema võimalikud huvid teostusjärgselt läbivaadatava IT-lahenduse suhtes ei kahjusta mitte mingil viisil läbivaatuse objektiivsust. Võimaliku huvide vastuolu korral tuleks sellest organisatsioonile selgelt teatada ning võimaluse korral tuleks enne ülesande vastuvõtmist organisatsioonilt saada kirjalik lausung selle kohta, et organisatsioon on vastuolust teadlik.

3.1.2 Kui IS audiitoril on või on olnud mingeid auditiväliseid rolle läbivaadatavas IT-lahenduses, peaks ta arvestama suunist G17 "Auditivälise rolli mõju IS audiitori sõltumatusele".

4 KUTSE-EETIKA JA STANDARDID

4.1 Teostuseelsed ja -järgsed läbivaatused

4.1.1 Erinevalt teostuseelsest läbivaatusest sooritatakse teostusjärgne läbivaatus harilikult siis, kui IT-lahendus on olnud kasutusel mingi mõistliku aja (harilikult mitme kuu või mitme protsessitsükli) kestel ning kasutajaprotseduurid ja rakendustaseme turvameetmed on teostatud.

4.1.2 Teostuseelsed läbivaatused uurivad meetmete ja haldusjälgede kontseptuaalset lahendust või nende tööd testkeskkonnas. Teostusjärgsed läbivaatused uurivad seda, kuidas meetmed ja haldusjäljed töötavad siis, kui IT-lahendus on installeeritud, konfigureeritud ja töötab tootmiskeskkonnas. Kui teostuseelne läbivaatus andis rahuldava tulemuse, peaks IS audiitor ise otsustama, kas piirduda teostusjärgsel läbivaatusel süsteemi tegeliku töö uurimisega tootmises.

4.1.3 Ressursside olemasolu puhul on eelistatav sooritada nii teostuseelne kui ka teostusjärgne läbivaatus, sest enne IT-lahenduse tegelikku teostamist võidakse viimasel hetkel teha muudatusi.

4.1.4 Teostusjärgse läbivaatuse sooritamisel peaks IS audiitor saama mõistliku kinnituse sellel, et läbivaatuse protsessis osalevad IT-lahenduse teostamise eest vastutav projekti omanik ja projekti töörühm. Töörühma liikmete hulka, keda küsitletakse läbivaatuse ühe osana, peaksid tavaliselt kuuluma

- IT-lahenduse kavandamise, väljatöötamise ja rakendamisega seotud inimesed;
- inimesed, kellel on töökogemus läbivaadataval alal ning seniste ja pakutavate äriprotsesside alal;
- asjassepuutuvate tehniliste teadmistega inimesed;

- inimesed, kes tunnevad organisatsiooni äristrateegiat ja teavad pakutud IT-lahenduse panust selle strateegia teostamisse;
- kasu realiseerumise protsessi mõõtmises ja seires osalejad.

5 PÄDEVUS

5.1 Oskused ja teadmised

5.1.1 IS audiitor peaks andma ka mõistliku kinnituse sellele, et tal on asjassepuutuvad oskused ja teadmised IT-lahenduse teostusjärgse läbivaatuse sooritamiseks. Kui on vajalikud asjatundjate teadmised, tuleks hankida sobiv teave.

6 PLAANIMINE

6.1 Läbivaatuse käsitlusala ja eesmärgid

6.1.1 IS audiitor peaks selgelt määratlema teostusjärgse läbivaatuse käsitlusala ja eesmärgid, pidades vajaduse korral nõu organisatsiooniga. Läbivaatusega kaetavad aspektid tuleksid selgelt sõnastada käsitlusala ühe osana.

6.1.2 Läbivaatuse eesmärkidel tuleks välja selgitada teostuse huvipooled.

6.1.3 Käsitlusala määramisel ja auditi plaanimisel tuleks arvestada IT-lahenduse või teostusprotsessi kõigi varasemate läbivaatuste (teostuseelsete või teostusaegsete) leide ja järeldusi.

6.2 Lähtetingimuste kinnitamine

6.2.1 Kui see vastab organisatsiooni tavadele, peaks IS audiitor saama lähtetingimustele ja metoodikale kinnituse asjassepuutuvatelt pooltelt organisatsioonis. Kui läbivaatuse algatab kolmas pool, tuleks saada lähtetingimuste kinnitus ka sellelt.

6.3 Metoodika

6.3.1 IS audiitor peaks sõnastama metoodika, millega saada mõistlik kinnitus sellele, et läbivaatuse käsitlusala ja eesmärke on võimalik saavutada objektiivselt ja professionaalselt. Metoodika tuleks asjakohaselt dokumenteerida. Metoodika ühe osana tuleks spetsifitseerida ka välistelt asjatundjatelt saadava teabe kasutamine. Teostusjärgsed läbivaatused ei piirdu esimesega pärast IT-lahenduse teostamist. Teostatud lahenduse edusammude väljaselgitamiseks võidakse sooritada mitu läbivaatust.

G29 Teostusjärgne läbivaatus (jätkub)

7 AUDITITÖÖ SOORITAMINE

7.1 Teostusjärgse läbivaatuse sooritamine

7.1.1 Teostusjärgne läbivaatus tuleks plaanida mingile mõistlikule ajale pärast IT-lahenduse teostamist. Sõltuvalt lahenduse tüübist ja ta keskkonnast võivad tüüpilised ajavahemikud ulatuda neljast nädalast kuue kuuni.

7.1.2 Teostusjärgne läbivaatus on mõeldud lõpliku töötava IT-lahenduse hindamise ja läbivaatusena. Korraliku läbivaatuse sooritamiseks peaks ideaaljuhul olema lõpetatud vähemalt üks teostuse ja aruandluse tsükkel. Läbivaatust ei tohiks sooritada seal ajal, kui tegeldakse alles esialgsete probleemide ja kasvuraskustega, ega ka siis, kui alles koolitatakse kasutajaid. Kui aga on võimalik, tuleks läbivaatus sooritada siis, kui on veel võimalik viia sisse viimaseid täiustusi, niie t IT-lahendusest saaks optimaalselt kasu.

7.1.3 Läbivaatuse protseduuride hulka peaksid kuuluma olemasoleva dokumentatsiooni (näiteks äriplaani, ärinõuete ja ärimeetmete, teostuvusuuringu, süsteemi-, käitus- ja kasutajadokumentatsiooni, edenemisaruannete, koosolekuprotokollide, kulu- ja tuluaruannete, testimis- ja koolitusplaanide ja --stsenaariumide jms) uurimine, arutelud huvipooltega, IT-lahenduse praktiline katsetamine ja lahendusega praktiline tutvumine, äri- ja projektipersonali vaatlemine ja küsitlemine ning käitus- ja juhtimisdokumentatsiooni uurimine.

7.1.4 Koostöös asjakohaste auditeeritava üksuse töötajatega tuleks välja selgitada ja eraldada teostusjärgse läbivaatuse sooritamiseks vajalikud ressursid ning plaanida läbivaatuse sooritamine.

7.1.5 Võimaluse korral tuleks kokku leppida teostusjärgse läbivaatuse tulemustest aruandmise vorm, sisu, adressaadid ja ajastus.

7.1.6 Detailselt tuleks uurida IT-lahenduse kohta deklareeritud eesmärke, kulusid ja tulusid. Tuleks hinnata nende eesmärkide saavutamise ulatust ning tegelikke kulusid ja tulusid, samuti protsesse ja süsteeme, millega hõivatakse, seiratakse ja teatatakse andmeid töötulemuste, kulude ja tulude kohta. Selle töö ühe osana tuleks uurida ka IT-lahendusega tekitatavaid tootlikkuse ja töötulemuste edusamme. Selles kontekstis tuleks kasutada sobivaid mõõtmiskriteeriume. Kui ilmneb ressursside ja/või aja ülekulu, tuleks seda analüüsida lähtudes selle põhjustest ja toimetest. Eraldi tuleks välja selgitada juhitavad ja mittejuhitavad põhjused.

7.1.7 IT-lahenduse määratlemiseks ja teostamiseks järgitud protsessi tuleks hinnata ta sobivuse ja toimivuse seisukohalt.

7.1.8 Tuleks läbi vaadata IT-lahenduse kasutajaile ja tugipersonalile antud koolituse adekvaatsus ja toimivus.

7.1.9 Tuleks uurida kõigi varasemate teostuseelsete või paralleelselt teostusprotsessiga sooritatud sisemiste või väljaspoolsete läbivaatuste aruandeid ning kontrollida soovituste ja rakendatud parandusmeetmete seisu.

G29 Teostusjärgne läbivaatus (jätkub)

7.1.10 Kuna teostusjärgne läbivaatus uurib IT-lahendust, peaks IT-lahendus üldiselt vastama asjakohastele COBITi juhtimiseesmärkidele. Asjassepuutuvatele juhtimiseesmärkidele vastavuse ulatust ja lahknevuste toimet tuleks analüüsida ja esitada tulemused aruandes. Peale selle tuleks läbivaadatavale IT-lahendusele ja teostusprotsessile sobivalt kohaldada COBITi juhtkonna suunistest kriitilisi edutegureid, keskseid sihiindikaatoreid ja küpsusmudeli mõõtlusnäitajaid.

7.1.11 Kogutud andmete, sooritatud analüüside, langetatud otsuste ja soovitatud parandusmeetmete kohta tuleks hoida käigus sobivad halduslikud kontrolljäljed.

7.1.12 Tuleks läbi vaadata, millises ulatuses vastavad IT-lahendus ja teostusprotsess põhikirja ja õigusaktide nõuetele ning organisatsiooni poliitikatele ja standarditele.

7.1.13 Sobivatel juhtudel võib IT-lahenduse asjassepuutuvate aspektide kontrollimiseks kasutada automatiseeritud testimisinstrumente ja CAAT-vahendeid.

7.1.14 Läbivaatus peaks tooma esile riskid ja probleemid, mis vajavad parandusmeetmeid, samuti võimalused meetmete täiustamiseks või teostusprotsessi toimivuse tõstmiseks.

7.1.15 Teatatud leiud, järeldused ja soovitused peaksid põhinema teostusjärgse läbivaatuse ajal saadud teabe ja asitõendite objektiivsel analüüsil ja tõlgendamisel.

8 KASU REALISEERUMISE LÄBIVAATUSED

8.1 Kasu realiseerumise läbivaatus

8.1.1 Kõik IT-projektid on tegelikult äriprojektid ja neil peaks algusest peale olema äriline põhjendus. Nende õnnestumist või ebaõnnestumist tuleks mõõta rahalises väljenduses või panusena strateegilise äriplaani elluviimisesse. Kasu realiseerumise läbivaatused peaksid keskenduma mitte ainult saavutatule, vaid ka sellele, mis tuleb veel teha. Organisatsioonid, kes korraldavad kasu realiseerimise läbivaatusi parimate tavade peenviimistluseks ja õppetundide saamiseks, lõikavad kasu oma järgmise projekti käsilevõtmisel.

8.2 Kasu realiseerumise läbivaatuse eesmärgid

8.2.1 Kasu realiseerumise läbivaatuse eesmärgid on hinnata uue IT-lahenduse töö edukust ning hinnata tegelikke kulusid, tulusid ja sääste võrreldes eelarvelistega. Läbivaatus võib uurida ka IT-lahenduse loomiseks ja teostuseks kasutatud protsessi toimivust. Üks keskseid küsimusi on selles, kas süsteemi algsed eesmärgid ja ajakavad saavutati. Et hinnata, millises ulatuses sihtprotsesside eesmärgid saavutati, tuleb üksikasjalikult tunda tegelikke ja sihtprotsesse.

8.2.2 Teostusjärgse läbivaatuse aruandes peaks kasu realiseerumise komponent käsitlema järgnevaid aspekte:

- tegelikud kulud võrreldes eelarvelistega;
- tegelik kasu võrreldes eelarvelisega;

- investeeringu tasuvus;
- tegelikud säästud võrreldes eelarvelistega;
- tegelikud projekti lõpetamise kuupäevad võrreldes plaanilistega;
- algsed eesmärgid võrreldes saavutatud eesmärkidega;
- dokumentatsiooni ja juhtimismeetmete, sealhulgas halduslike kontrolljälgede adekvaatsuse hindamine;
- IT-lahenduse tegelikud töötulemused võrreldes oodatud tulemustega;
- kasutajate üldine rahulolu uue IT-lahenduse süsteemiga ja selle süsteemi tundmine;
- ettepanekud töötulemuste parandamiseks tulevastes IT-lahenduste teostamise projektides.

9 VÄLJASTTELLIMINE

9.1 IT väljasttellimine

9.1.1 Kui organisatsioon on oma IT-lahenduse teostamise või osa sellest täielikult või osaliselt delegeerinud mingile välisele selliste teenuste andjale (teenuseandjale), peaks IS audiitor hindama sellise korralduse toimet ning kontrollima teenuseandjaga sõlmitud lepingute, kokkulepete ja õigusaktide adekvaatsust ning nende järgimist.

9.1.2 IS audiitor peaks õppima tundma väljasttellitavate teenuste iseloomu, ajastust ja ulatust. IS audiitor peaks ka välja selgitama, milliseid meetmeid rakendab teenuseandja organisatsiooni ärinõuete ja organisatsiooni poolt nõutavate meetmete täitmiseks (vt suunis G4 "IS-tegevuste tellimine teistelt organisatsioonidelt".

10 ARUANDLUS

10.1 Aruande sisu

10.1.1 Teostusjärgse läbivaatuse aruandes peaksid sõltuvalt läbivaatuse eesmärkidest ja käsitlusalast olema esitatud järgmised aspektid:

- käsitlusala, eesmärgid, järgitud metoodika ja aluseks võetud eeldused;
- hinnang selle kohta, kas IT-lahenduse teostamisele kavandatud eesmärgid on saavutatud ja kas IT-lahendused on suunatud ärieesmärkide saavutamisele;
- teostusprotsessi üldine hinnang kesksete tugevate ja nõrkade külgede väljenduses ning nõrkuste tõenäoline toime;
- soovitused oluliste nõrkuste kõrvaldamiseks ja teostusprotsessi täiustamiseks;
- potentsiaalsed riskid ja nende leevendamise vahendid;

G29 Teostusjärgne läbivaatus (jätkub)

- COBITi teabekriteeriumidele vastavuse ulatus;
- soovitused tulevaste IT-lahenduste ja teostusprotsesside täiustamiseks;
- teostatud IT-lahenduse kasutajate koolitus;
- IT-lahenduste omaksvõtt ja sobitatavus kogu organisatsioonis.

10.1.2 Leiud ja soovitused tuleks vastavalt vajadusele kooskõlastada huvipooltega ja organisatsiooniga (ja vajaduse korral teenuseandjaga) ning saada neilt tagasisidet enne aruande viimistlemist.

10.2 Nõrkused

10.2.1 Teostusjärgse läbivaatuse käigus tuvastatud nõrkused, mis on tingitud juhtimismeetmete puudumisest, protsesside halvast teostusest või kaasnevate riskide leevendamata jätmisest vastuvõetavate suurusteni, tuleks teha teatavaks äriprotsessi omanikule ja IT-lahenduse teostamise eest vastutavale IS juhtkonnale. Kui teostusjärgse läbivaatuse käigus tuvastatud nõrkusi loetakse olulisteks või kaalukateks, tuleks aegsaks parandusmeetmete rakendamiseks viivitamatult pidada nõu juhtkonna asjakohase tasemega.

10.2.2 Kuna IT-lahendustele rakendatavate meetmete toimivus sõltub üldistest IT-meetmetest, tuleks teatada ka kõigist nõrkustest nende alal. Kui üldisi IT-meetmeid ei uuritud, tuleks see asjaolu märkida aruandesse.

10.2.3 IS audiitor peaks aruandesse paigutama sobivad meetmete tugevdamise soovitused kaasnevate riskide leevendamiseks.

11 JÄRELTOIMINGUD

11.1 Õigeaegsus

11.1.1 Kõigi teostusjärgse läbivaatusega avastatud nõrkuste toimed on tõenäoliselt laiaulatuslikud ja tekitavad suuri riske. Seetõttu peaks IS audiitor vajaduse korral sooritama piisava ja õigeaegse järeltöö kontrollimaks, kas nõrkuste käsitlemiseks ja riskide toimivaks halduseks on rakendatud haldusmeetmeid.

12 JÕUSTUMISKUUPÄEV

12.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. jaanuaril 2005 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

Allikaviide

IS auditeerimise suunis G23 "Süsteemi arengu elutsükli (SDLC) läbivaatused"

G30 Pädevus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S4 "Kutsealane pädevus" määrab: "IS audiitor peaks olema kutsealaselt pädev, tal peaksid olema auditiülesande täitmiseks vajalikud oskused ja teadmised. IS audiitor peaks asjakohase pideva kutsealase õppe ja koolitusega hoidma ülal oma kutsealast pädevust."

1.2 Seos COBITiga

1.2.1 Lai juhtimiseesmärk S3 ("Saada sõltumatu kinnitus", COBIT v3) määrab: "... saada sõltumatu kinnitus organisatsioonide, klientide ja kolmandatest pooltest tarnijate vahelise usalduse ja usaldusväärsuse suurendamiseks."

1.2.2 Lai juhtimiseesmärk S4 ("Korraldada sõltumatu audit", COBIT v3) määrab: "... korraldada sõltumatu audit usalduse suurendamiseks ja parimate tavade alastest nõuannetest kasu saamiseks."

1.2.3 Detailne juhtimiseesmärk S3.7 ("Sõltumatu kinnituse talituse pädevus", COBIT v3) määrab: "Juhtkond peaks tagama, et sõltumatu kinnituse talitusel on tehniline pädevus, oskused ja teadmised, mis on vajalikud selliste läbivaatuste toimivaks, tõhusaks ja ökonoomseks sooritamiseks."

1.2.4 Detailne juhtimiseesmärk S4.4 ("Pädevus", COBIT v3) määrab: "Juhtkond peaks tagama, et organisatsiooni IT-tegevuste läbivaatuse eest vastutavad audiitorid on tehniliselt pädevad ja et neil on kollektiivselt oskused ja teadmised (st CISA valdkondades), mis on vajalikud selliste läbivaatuste toimivaks, tõhusaks ja ökonoomseks sooritamiseks. Juhtkond peaks tagama, et infosüsteemide auditeerimise töödele määratud auditipersonal säilitaks tehnilise pädevuse pideva sobiva koolituse teel."

1.3 Toetumine COBITile

1.3.1 Toetumine COBITile pakub spetsiifilisi COBITi eesmärke või protsesse, mida tuleks arvestada selles suunises käsitletava ala läbivaatusel. Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ning arvestades COBITi teabekriteeriume ja nendega seotud juhtimistavasid. Selle nõude täitmiseks on COBITist valitud ja sobitatud tõenäoliselt kõige asjakohasemad protsessid ning need on alljärgnevas liigitatud esma- ja teisejärgulisteks. Valitavad ja sobitatavad juhtimiseesmärgid võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest.

1.3.2 Esmajärgulised

- PO7 – Hallata IT inimressursse
- S2 – Hinnata sisejuhtimise adekvaatsust (COBIT v3)

- S3 – Saada sõltumatu kinnitus (COBIT v3)
- S4 – Korraldada sõltumatu audit (COBIT v3)

1.3.3 Teisejärgulised

- TT1 – Määratleda teenusetasemed ja hallata neid
- TT2 – Hallata kolmandate osapoolte teenuseid
- TT3 – Hallata suutlikkust ja võimsust
- TT7 – Koolitada kasutajaid
- SH1 – Seirata ja hinnata IT töötulemusi

1.3.4 Pädevuse puhul kõige asjassepuutuvamad on järgnevad teabekriteeriumid:

- esmajärjekorras: toimivus, tõhusus ja käideldavus;
- teises järjekorras: konfidentsiaalsus, terviklus, vastavus ja usaldatavus.

1.4 Suunise eesmärk

1.4.1 IS audiitoreilt oodatakse suurt pädevust. Selle eesmärgi saavutamiseks tuleb IS audiitoritel omandada ülesannete täitmiseks vajalikud oskused ja teadmised. Lisaks sellele tuleb neil säilitada oma pädevus teadmiste ja oskuste pideva täiendamise teel.

1.4.2 IS audiitorite nõustumine anda kutsealaseid teenuseid laseb järeldada, et neil on kutsealaste teenuste andmiseks vajalik soovitav pädevustase ning et IS audiitori teadmisi ja oskusi rakendatakse asjakohase hoolikuse ja tähelepanelikkusega.

1.4.3 Niisuguste suure pädevuse ootuste tõttu peaksid IS audiitorid loobuma kõigi selliste teenuste andmisest, mida nad ei ole pädevad andma, kui nad ei saa nõu ja abi, mis võimaldab mõistlikult kinnitada, et teenused tehakse teoks rahuldavalt.

1.4.4 IS audiitor peaks andma kutsealaseid teenuseid asjakohase hoolikuse, pädevuse ja tähelepanelikkusega ning ta pidev kohustus on hoida kutsealased teadmised ja oskused vajalikul tasemel, andes mõistliku kinnituse sellele, et kutsealaste auditeerimise standardite nõuded täidetakse ning et auditeeritav organisatsioon saab hüvena kasutada pädevat kutsealast teenust, mis põhineb uusimatel tavade, õigusnormide ja meetodite arengutel.

1.4.5 ISACA deklareeritud visioon on olla IT halduse, juhtimise ja tagamise ala tunnustatud ülemaailmne liider. Visiooni eessõnas on selgelt rõhutatud, et ISACA teenindatavate kutsealade tulevane edu nõuab oskusi ja pädevusi, mis täiendavad CISA tiitliga mõõdetavaid. ISACA on esirinnas niisuguste oskuste ja pädevuste piiritlemisel ning nende kvantiteerimise ja mõõtmise viiside väljatöötamisel. Just niisuguses kontekstis vajatakse suunist, mis annaks IS audiitoritele juhiseid vajalike oskuste ja teadmiste omandamiseks ja pädevuse säilitamiseks auditiülesannete täitmisel.

G30 Pädevus (jätkub)

1.4.6 See suunis annab juhiseid IS auditeerimise standardi S4 "Kutsealane pädevus" rakendamiseks. IS audiitor peaks seda suunist arvestama otsustamisel, kuidas saavutada nimetatud standardi rakendamine, kasutama suunise rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama kõiki lahknevusi.

1.5 Suunise rakendamine

1.5.1 Selle suunise rakendamisel peaks IS audiitor arvestama ta juhiseid seostatult muude asjassepuutuvate ISACA standardite ja suunistega.

2 VASTUTUS

2.1 Oskused ja teadmised

2.1.1 Eelkõige peaks IS audiitor vastutama selle eest, et ta omandab vajalikud kutsealased ja tehnilised oskused ja teadmised kõigi nende ülesannete täitmiseks, mida ta nõustub täitma.

2.1.2 Teiseks vastutab auditi juhtkond selle eest, et usaldab auditi ülesande IS audiitorile alles pärast veendumist selles, et IS audiitoril on tööde tegemiseks vajalikud kutsealased ja tehnilised oskused ja teadmised.

2.1.3 Auditi juhtkonna kohus on veenduda, et auditit sooritava rühma liikmetel on nõutavad oskused ja teadmised.

2.1.4 Vajalikud oskused ja teadmised sõltuvad IS audiitori positsioonist ja rollist auditi suhtes. Juhtimisoskuste ja -teadmiste nõue peaks olema proportsioonis vastutustasemega.

2.1.5 Oskuste ja teadmiste hulka kuuluvad oskused ja teadmised riskide ja meetmete väljaselgitamise ja haldamise alal ning auditi vahendite ja meetodite alal. IS audiitoril peaksid olema analüütilised ja tehnilised teadmised ning oskused küsitlemise, inimsuhete ja ettekannete alal.

2.2 Pädevus

2.2.1 Pädevus eeldab adekvaatse haridustasemega ja kogemustega omandatud oskusi teadmisi ja asjatundlikkust.

2.2.2 IS audiitor peaks andma mõistliku kinnituse sellele, et tal on nõutaval pädevustasemel olemiseks vajalikud oskused ja teadmised.

2.2.3 IS audiitor peaks kavandama soovitava ja/või oodatava pädevustaseme sobivate mõõtlusnäitajate põhjal ning neid näitajaid tuleks perioodiliselt läbi vaadata ja ajakohastada.

2.2.4 Enne auditiülesande vastuvõtmist peaks IS audiitor ja/või auditi juhtkond andma mõistliku kinnituse selle kohta, et iga auditiülesande täitmiseks on olemas vajalikud pädevad ressursid ning enne auditi alustamist tuleks tõendada selliste pädevate ressursside olemasolu.

2.2.5 Auditi juhtkonna kohus on tagada, et töörühma liikmed oleksid pädevad täitma auditiülesannet. Rühma liikmete põhipädevuste piiritlemine aitab olemasolevaid ressursse tõhusalt ära kasutada.

2.2.6 Ressursside pädevuse tõstmiseks peetakse sobivaks, et IS audiitorid jagaksid rühma liikmete vahel oma kogemusi, omaksvõetud parimaid tavasid, saadud õppetunde ja omandatud teadmisi.

2.3 Taseme pidev säilitamine

2.3.1 Aktsepteeritava pädevustaseme säilitamiseks peaks IS audiitor pidevalt jälgima oma oskusi ja teadmisi.

2.3.2 Säilitamine pideva kutseõppe (CPE) kaudu võib hõlmata (ja mitte ainult) koolitust, täienduskursusi, sertifitseerimisprogramme, ülikooli, konverentse, seminare, mõttekodasid, kaugnõupidamisi, veebiloenguid ja õpperingide koosolekuid.

2.3.3 Oskuste ja teadmiste omandamist ja pädevustasemete säilitamist tuleks pidevalt seirata ning selliseid oskusi, teadmisi ja pädevusi tuleks perioodiliselt hinnata.

2.4 Hindamine

2.4.1 Hindamine tuleks sooritada nii, et see oleks õiglane, läbipaistev, arusaadav, ühemõtteline, nihketa ja konkreetse töökeskkonna puhul üldaktsepteeritavaks tavaks peetav.

2.4.2 Hindamiskriteeriumid ja protseduurid peaksid olema selgelt määratletud, kuid nad võivad varieeruda sõltuvalt sellistest asjaoludest nagu geograafiline asukoht, poliitiline kliima, ülesande iseloom, kultuur jms tingimused.

2.4.3 Auditifirma või audiitorite töörühma puhul tuleks hindamine sooritada sisemisena töörühmade hulgas või isikute hulgas talitustevahelisena.

2.4.4 Sõltumatu IS üksikaudiitori puhul tuleks hindamine sooritada võimalikult suures ulatuses võrdpartnerluse alusel. Kui partnerläbivaatus ei ole võimalik, tuleks sooritada ja dokumenteerida enesehindamine.

2.4.5 IS siseaudiitori, vajaduse ja võimaluse korral ka IS välisaudiitori(te) töösoorituse hindamiseks on vajalik sobiv juhtkonna tase.

2.4.6 Hindamise käigus ilmnenud lünkadega tuleb asjakohaselt tegeleda.

G30 Pädevus (jätkub)

2.5 Lünkade analüüs ja koolitus

2.5.1 Tegeliku pädevustaseme ja oodatava pädevustaseme vaheliste lahknevuste põhjal avastatud lüngad tuleks registreerida ja neid tuleks analüüsida. Kui mingis ressursis on puudusi, ei tohiks seda ressurssi kasutada auditiülesande täitmiseks, kuni ei ole rakendatud adekvaatseid meetmeid puuduste kõrvaldamiseks. Kui aga puudust märgatakse pärast auditiülesande täitmise alustamist, peaks IS audiitor või auditi juhtkond mõtlema puudulike ressursside kõrvaldamisele ja nende asendamisele pädevate ressurssidega. Kui ollakse sunnitud jätkama sellise ressursi kasutamist auditi jätkamiseks, tuleks lünga olemasolust teatada auditeeritavale. Kui IS audiitor suudab mõistlikult tagada auditi kvaliteeti, tuleks puuduliku ressursi kasutamise jätkamisele saada auditeeritava nõusolek.

2.5.2 Oluline on sooritada lünga põhjuse väljaselgitamiseks algpõhjuse analüüs ning rakendada võimalikult kiiresti sobivaid parandusmeetmeid, näiteks koolitust.

2.5.3 Auditiülesandeks vajalik koolitus tuleks läbi viia mõistliku ajaga ja enne audititegevuse alustamist.

2.5.4 Pärast koolituse lõppu tuleks mingi mõistliku aja pärast mõõta koolituse toimivust.

2.6 Pädevate ressursside olemasolu

2.6.1 IS audiitor ja/või auditi juhtkond peaks ennepakkumiskutsele vastamist tundma ja analüüsima pakutava auditiülesande oskuste ja teadmiste vajadust.

2.6.2 Enne auditiülesannete täitmise alustamist peaks IS audiitor ja/või auditi juhtkond andma mõistliku kinnituse sellele, et nõutavad ressursid vajalike oskuste, teadmiste ja pädevustasemetega on olemas.

2.6.3 IS audiitorid ei tohiks endale omistada sellist asjatundmist, pädevust ega kogemust, mida neil ei ole.

2.7 Väljasttellimine

2.7.1 Kui mingi osa auditiülesande täitmisest tellitakse väljastpoolt või saadakse abi asjatundjailt, tuleb saada mõistlik kinnitus sellele, et välisel asjatundjal või väljasttellimiseks kasutataval asutusel on nõutav pädevus. See suunis kehtib ka välise asjatundja valimise puhul.

2.7.2 Kui asjatundjate abi hangitakse pidevalt, tuleks selliste väliste asjatundjate pädevust perioodiliselt mõõta ja seirata või läbi vaadata.

G30 Pädevus (jätkub)

3 PIDEV KUTSEÕPE (CPE)

3.1 Kutsealakogude nõuded

3.1.1 Pidev kutseõpe (CPE) on metoodika, mida rakendatakse pädevuse säilitamiseks ning oskuste ja teadmiste ajakohastamiseks.

3.1.2 IS audiitorid peaksid järgima oma kutsealakogude kehtestatud CPE poliitikate nõudeid.

3.2 Kõlblikud programmid

3.2.1 CPE programmid peaksid aitama suurendada oskusi ja teadmisi ning olema kooskõlas IS tagamise, turbe ja halduse kutsealaste ja tehniliste nõuetega.

3.2.2 Harilikult kirjutavad kutsealakogud ette programmid, mis on kõlblikud tunnustamiseks CPE järgi. IS audiitorid peaksid järgima selliseid oma kutsealakogude määratud norme.

3.3 CPE-tunnustuse saamine

3.3.1 Kutsealakogud kirjutavad harilikult ette CPE-tunnustuse saamise metoodika ja minimaalse tunnustuse, mille peavad regulaarselt saama nende liikmed. IS audiitorid peavad järgima selliseid oma kutsealakogu ettekirjutatud norme.

3.3.2 Kui IS audiitor on seotud mitme kutsealakoguga, võib ta minimaalse tunnustuse saamiseks ise otsustada saada CPE-tunnustuse tavalisel viisil, kõlblike programmide kaudu, kui see on kooskõlas vastavate kutsealakogude kehtestatud eeskirjade või suunistega.

3.4 ISACA CPE-poliitika

3.4.1 ISACA kohaldab oma liikmetele ja CISA nimetuse kandjaile laiaulatuslikku pideva kutseõppe poliitikat. CISA nimetusega IS audiitorid peavad järgima ISACA CPE-poliitikat. Selle poliitika üksikasju võib leida ISACA veebisaidist aadressil *http://www.isaca.org/CISAcpePolicy*. See poliitika seletab kriteeriume alljärgneva kohta:

- sertifitseerimisnõuded,
- osavõtuvormi tõendamine,
- kutse-eetika koodeks,
- pideva kutseõppe aegade auditid,
- tühistamine, ümberotsustus ja edasikaebus,
- ametist lahkunud ja mittepraktiseeriva CISA staatus,

G30 Pädevus (jätkub)

- koolitustegevuste kvalifitseerimine,
- pideva kutseõppe tundide arvutus.

4 ANDMIKUD

4.1 Oskuste maatriks ja koolitusandmikud

4.1.1 Tuleks koostada oskuste maatriks, mis näitab mitmesuguste töö tasemete jaoks nõutavaid oskusi, teadmisi ja pädevusi. Selles maatriksis peaksid olema vastastikused viited olemasolevatele ressurssidele ning nende oskustele ja teadmistele. See maatriks aitab tuvastada lünki ja koolitusvajadusi.

4.1.2 Sooritatud koolituste andmikud koos koolituse ja selle toimivuse kohta saadud tagasisidega tuleks säilitada, neid tuleks analüüsida viitestada tulevaseks kasutamiseks.

4.2 CPE andmikud

4.2.1 Vastavate kutsealaste kogude, sealhulgas ISACA ettekirjutuste kohaselt peavad IS audiitorid pidama CPE programmide kohta asjakohaseid andmikke, säilitama neid teatud aja kestel ning vajaduse korral tegema nad kättesaadavaks audititele.

5 JÕUSTUMISKUUPÄEV

5.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. juunil 2005 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

G31 Privaatsus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S1 "Audititalituse põhikiri" määrab: "Infosüsteemide auditi talituse või infosüsteemide auditi ülesande eesmärk, kohustused, õigused ja vastutus peaksid olema auditi põhikirjas või töövõtukirjas asjakohaselt dokumenteeritud."

1.1.2 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.3 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.2 Seos COBITiga

1.2.1 Lai juhtimiseesmärk SH3 "Tagada vastavus välisnõuetele" määrab: "Välisnõuetele vastavuse tagamise IT protsessi juhtimist, mis rahuldab ärinõuet täita seaduste, eeskirjade ja lepingutega pandud kohustused, võimaldab välisnõuete toime väljaselgitamine ja analüüsimine ning sobivate meetmete rakendamine nende nõuete täitmiseks, võttes arvesse

- seadused, eeskirjad ja lepingud,
- seaduste ja eeskirjade arengu seire,
- vastavuse regulaarse seire,
- ohutuse ja ergonoomia,
- privaatsuse,
- intellektuaalse omandi."

1.2.2 Detailne juhtimiseesmärk PO8.4 "Privaatsus, intellektuaalne omand ja andmete liikumine" määrab: "Juhtkond peaks tagama vastavuse privaatsust, intellektuaalset omandit, riigipiire ületavaid andmevooge ja krüptograafiat puudutavatele õigusaktidele, mis on kohaldatavad organisatsiooni infotehnoloogiatavadele."

1.3 Toetumine COBITile

1.3.1 Käesolevas suunises käsitletava ala läbivaatusel tuleks arvestada COBITi spetsiifilisi eesmärke või protsesse järgneva põhjal. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ning COBITi juhtimiseesmärkide ja nendega seotud juhtimistavade arvestamisel. Privaatsuse küsimuses on kõige tõenäolisemalt asjakohastena valitavad ja kohaldatavad COBITi protsessid alljärgnevas loetelus jagatud esmasteks ja teisesteks. Protsessid ja juhtimiseesmärgid, mis tuleb valida, võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest.

G31 Privaatsus (jätkub)

1.3.2 Esmajärjekorras

- PO8 – Tagada vastavus välisnõuetele (COBIT v3)
- TT5 – Tagada süsteemide turvalisus

1.3.3 Teises järjekorras

- PO7 – Hallata IT inimressursse
- TT1 – Määratleda teenusetasemed ja hallata neid
- TT2 – Hallata kolmandate osapoolte teenuseid
- TT10 – Hallata probleeme
- TT11 – Hallata andmeid
- TT13 – Hallata käitust
- SH1 – Seirata ja hinnata IT töötulemusi
- SH2 – Seirata ja hinnata sisejuhtimist
- S3 – Saada sõltumatu kinnitus (COBIT v3)
- S4 – Korraldada sõltumatu audit (COBIT v3)

1.3.4 Privaatsuse läbivaatuse jaoks kõige asjakohasemad teabekriteeriumid on

- esmajärjekorras toimivus, vastavus, konfidentsiaalsus ja terviklus;
- teises järjekorras usaldatavus ja käideldavus.

1.4 Suunise eesmärk

1.4.1 Selle suunise eesmärk on aidata IS audiitoril mõista privaatsust ja IS auditi ülesannete täitmisel käsitleda privaatsuse küsimusi asjakohaselt. See suunis on eeskätt suunatud IS auditi talitusele, kuid selle aspekte võib arvestada ka muudes olukordades.

1.4.2 See suunis annab juhiseid IS auditeerimise standardite rakendamiseks. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardi elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

1.5 Suunise rakendamine

1.5.1 Selle suunise rakendamisel peaks IS audiitor arvestama ta juhiseid seotult muude asjassepuutuvate ISACA standardite ja suunistega.

G31 Privaatsus (jätkub)

1.6 Privaatsuse määratlus IS auditeerimise kontekstis. Kitsendused ja kohustused

1.6.1 Privaatsus tähendab usalduse ja kohustuste järgimist igasuguse teabe puhul, mis on seotud mingi identifitseeritud või identifitseeritava üksikisikuga (andmesubjektiga). Juhtkonna kohus on järgida privaatsust vastavalt oma privaatsuspoliitikale või kohaldatavatele privaatsust puudutavatele õigusaktidele.

1.6.2 Isikuandmed on igasugune teave, mis on seotud mingi identifitseeritud või identifitseeritava üksikisikuga.

1.6.3 IS audiitor ei vastuta selle eest, mida talletatakse isikuandmebaasides, ta peaks kontrollima, kas isikuandmeid hallatakse õigusnormide suhtes õigesti ja rakendades õigeid turvameetmeid.

1.6.4 IS audiitor peaks läbi vaatama juhtkonna privaatsuspoliitika, veendumiseks, et see võtab arvesse kohaldatavad privaatsust puudutavate õigusaktide nõuded, sealhulgas nõuded piire ületavatele andmevoogudele, näiteks programmi "Safe Harbour" põhimõtted ning OECD suunised isikuandmete privaatsuse ja piire ületavate andmevoogude kaitse kohta.

1.6.5 IS audiitorid peaksid läbi vaatama juhtkonna sooritatud privaatsuse mõju analüüsi või hindamise. Sellised hindamised peaksid

- selgitama välja tegevusprotsessidega seotud isikupõhise teabe iseloomu;
- dokumenteerima isikupõhise teabe kogumise, kasutamise, avaldamise ja hävitamise;
- andma juhtkonnale vahendi, millega teha poliitikate, käituse ja süsteemide kavandamise kohta informeeritud otsuseid, mis põhinevad privaatsusriski ja selle leevendamise võimaluste tundmisel;
- andma mõistliku kinnituse sellele, et privaatsusküsimustes on olemas jälitatavus;
- looma järjekindla vormingu ja struktureeritud protsessi, millega analüüsida nii tehnilist kui ka juriidilist vastavust asjassepuutuvatele õigusaktidele;
- vähendama läbivaatusi ja viima infosüsteeme vastavusse privaatsusnõuetega;
- looma raamstruktuuri, millega tagada, et privaatsust arvestatakse algatamise ja nõuete analüüsi järgust kuni lõpliku lahenduse kinnitamise, rahastamise, teostuse ja teatavaks tegemise järguni.

1.6.6 IS audiitorid peaksid selgitama välja, kas neid hindamisi viiakse läbi privaatsuse algse läbivaatuse osana ning seejärel regulaarselt iga muudatuste halduse projekti puhul, mille sisuks on näiteks

- muudatused tehnoloogias;
- uued programmid või suured muudatused olemasolevates;
- süsteemide lisasidemed;
- kättesaadavuse suurendamine;

- talitlusprotsessi ümberrajamine;
- andmeaidastus;
- uued tooted, teenused, süsteemid, operatsioonid, tarnijad ja äripartnerid.

1.6.7 Kui IS audiitorid kaalutlevad kohaldatavaid privaatsust puudutavaid õigusakte, mida tuleb järgida igas organisatsioonis, eriti aga organisatsioonides, mis tegutsevad maailma eri osades, peaksid nad küsima asjatundjate arvamust õigusaktide nõuete kohta ning sooritama vajalikud vastavuse ja olulisuse kontrollimised arvamuse kujundamiseks ja aruandluseks sellistele õigusaktidele vastavuse kohta.

1.6.8 Andmevalitseja on osapool, kes on pädev tegema otsuseid isikuandmete sisu ja kasutamise kohta, sõltumata sellest, kas ta ise otseselt või vahendaja kaudu kogub, talletab, töötleb või levitab selliseid andmeid või ei tee seda.

2 AUDITI PÕHIKIRI

2.1 Privaatsus kokkuühendatud maailmas

2.1.1 WWW, elektronposti jms sidetehnoloogia areng võimaldab teavet tõhusalt levitada ülemaailmses ulatuses. Tuleks rakendada meetmeid, millega tagada selle tehnoloogia ning elektroonilisel, digiteeritud või paberkujul isikuteabe esituse eetiline kasutamine. Peale selle nõuab õigusaktide ülemaailmne jõustamine organisatsioonidelt meetmete rakendamist isikute privaatsuse kaitseks. See suunis annab ühe üldise kriteeriumide kogumi, mida IS audiitor saab rakendada nende turvameetmete hindamiseks, mis on mõeldud tagama inimeste privaatsust.

3 SÕLTUMATUS

3.1.1 Teabeallikad

3.1.1 Audiitor peaks arvestama organisatsioonis rakendatavaid kohalikke õigusakte privaatsuse kohta, seejärel aga ülemaailmseid. Kui organisatsioon on rahvusvaheline, peaks ta arvestama, et kohalikel õigusaktidel on prioriteet ettevõtte poliitikate ees, kuid praegusel juhul peab organisatsioon peale selle järgima mõlemat (näiteks Sarbanes-Oxley seadust USA firmade puhul).

4 KUTSE-EETIKA JA STANDARDID

4.1 Isikuandmete kaitse vajadus

4.1.1 Üha suurem arv ühendusi sisemiste ja väliste andmekogude või -allikate vahel ning Interneti kasutamine suurendavad privaatsuse vajadust nii avalikus sektoris kui ka eraettevõtetes. Elu, tervist, majanduslikku olukorda, seksuaalset seadumust, religiooni, poliitilisi vaateid jms puudutava teabe avaldamine kõrvalistele isikutele võib inimestele tekitada parandamatut kahju.

G31 Privaatsus (jätkub)

4.1.2 Paljudes maades on olemas privaatsust puudutavad õigusaktid, kuid sageli ei tunta neid või ei ole nad piisavalt spetsiifilised. Seetõttu peavad IS audiitoril olema algteadmised privaatsuse küsimustes ning ettevõtte isikuteabe kaitse taseme hindamiseks peab ta vajaduse korral teadma põhilisi erinevusi eri maade õigusnormides.

5 PÄDEVUS

5.1 Isikuandmete kaitse metoodika

5.1.1 Isikuandmete konfidentsiaalsuse, tervikluse ja käideldavuse kindlustamiseks peavad olema kehtestatud nõuded ja reeglid digiteeritud ja paberkujul isikuteabe käsitlusele. Igal organisatsioonil peab olema mingi metoodika igat liiki ja igal kujul isikuteabe kaitsmiseks ning ta peaks võtma arvesse alljärgneva.

- Privaatsuse haldus. Eelkõige vastutab privaatsuse eest tegevdirektor või organisatsiooni juhtiv isik. Isikuteabe kasutamise eesmärk ja olulised üldised suunised peaksid olema kirjeldatud turvaeesmärkides, -poliitikas ja -strateegias. Sagedaseks hindamiseks peaksid olema formaliseeritud menetlused, millega saada mõistlik kinnitus sellele, et isikuteabe kasutamine vastab organisatsiooni vajadustele ning üldkehtivatele õigusaktidele. Hindamise tulemused tuleks dokumenteerida ning kasutada turvapoliitika ja -strateegia võimaliku muutmise alusena.
- Riski kaalutlemine. Organisatsioonil peaks olema ülevaade kasutatava isikuteabe mitmesugustest liikidest. Organisatsioon peaks ka määrama kriteeriumid isikuandmete käsitlusega seotud aktsepteeritavale riskile. Vastutus isikuteabe eest tuleks panna "andmerevidendile". Andmevalitseja vastutab turvaintsidentide tõenäosuse ja tagajärgede väljaselgitamiseks mõeldud riskikaalutlemiste sooritamise eest. Uued riski kaalutlemised tuleks sooritada vastavalt informatsiooni turvalisuse tähtsuse muutustele. Riski kaalutlemiste tulemused tuleks dokumenteerida.
- Turvaaudit. Infosüsteemide kasutamist puudutavaid turvaauditeid tuleks sooritada regulaarselt. Turvaaudit peaks hõlmama organisatsiooni, turbetaotlusi ning koostööd partnerite ja tarnijatega. Tulemused tuleks dokumenteerida.
- Lahknevused. Igasugust infosüsteemide kasutamist, mis ei vasta formaliseeritud menetlustele ja mis võib põhjustada turvarikkeid, tuleks käsitleda lahknevusena. Lahknevuste käsitlemise eesmärk on taastada normaalsed tingimused, kõrvaldada lahknevuseni viinud põhjus ja vältida lahknevuse kordumist. Kui lahknevused on põhjustanud konfidentsiaalse teabe volitamatut avaldamist, tuleb sellest võib-olla teatada kohalikele ametivõimudele. Tulemused tuleks dokumenteerida.
- Organisatsioon. Tuleks kehtestada ja dokumenteerida vastutus infosüsteemide kasutamise eest. Vastutus peaks olema muutumatu ilma asjakohase juhtkonna loata. Infosüsteem tuleks konfigureerida saavutama rahuldavat teabe turvalisust. Konfiguratsioon tuleks dokumenteerida ja teda tuleks muuta ainult asjakohase juhtkonna loal.

G31 Privaatsus (jätkub)

- Personal. Töötajad peaksid kasutama isikuteavet vastavalt oma tööülesannetele ja neil peaks olema selleks vajalik luba. Peale selle peaksid töötajail olema vajalikud teadmised infosüsteemi kasutamiseks vastavalt formaliseeritud menetlustele. Infosüsteemide lubatav kasutamine tuleks registreerida.
- Kutsealane salastus. Töötajad peaksid alla kirjutama formaalse leppe selle kohta, et nad ei avalda mitte mingisugust isikuteavet, kui konfidentsiaalsus on vajalik. See salastus peaks hõlmama ka muud teavet, mis on teabe turvalisuse seisukohalt oluline.
- Füüsiline turve. Organisatsioon peaks rakendama meetmeid volitamata juurdepääsu välistamiseks tehnilistele seadmetele, mida kasutatakse isikuteabe töötluseks. Turvameetmed peaksid hõlmama ka muid seadmeid, mis on teabe turvalisuse seisukohalt olulised. Seadmed tuleks installeerida nii, et see ei mõjutaks isikuteabe käsitlust.
- Konfidentsiaalsus. Ettevõte peaks rakendama meetmeid volitamata juurdepääsu välistamiseks isikuteabele, kui konfidentsiaalsus on vajalik. Turvameetmed peaksid välistama volitamata juurdepääsu ka muule teabele, mis on teabe turvalisuse seisukohalt oluline. Välistele partneritele elektrooniliselt edastatav konfidentsiaalne isikuteave tuleks krüpteerida või muul viisil turvata. Konfidentsiaalset isikuteavet sisaldav talletatav teave tuleks asjakohaselt märgistada.
- Terviklus. Isikuandmete volitamata muutmise tõrjeks tuleks rakendada meetmeid, millega mõistlikult tagada terviklus. Turvameetmed peaksid välistama volitamata muutmise ka muu teabe puhul, mis on teabe turvalisuse seisukohalt oluline. Peale selle tuleks rakendada meetmeid kahjurtarkvara tõrjeks.
- Käideldavus. Tuleks rakendada meetmeid isikuteabele juurdepääsu mõistlikuks tagamiseks. Turvameetmed peaksid hõlmama ka muud teavet, mis on teabe turvalisuse seisukohalt oluline. Teabele juurdepääsu mõistlikuks kindlustamiseks olukordades, kus normaalne talitlus ütleb üles, peaksid olema käigus varunduse ja taaste menetlused. Tuleks kehtestada korralikud varunduse menetlused.
- Turvameetmed. Tuleks rakendada turvameetmeid infosüsteemide volitamata kasutamise välistamiseks ja volitamata juurdepääsu katsete avastamiseks. Kõik volitamata juurdepääsu katsed tuleks logida. Turvameetmed peaksid hõlmama abinõusid, mida personal ei saa mõjutada ega ületada ning ei tohiks piirduda isikute vastu rakendatavate õiguslike meetmetega. Turvameetmed tuleks dokumenteerida.
- Turve välispartnerite suhtes. Kohustuste ja õiguste selgitamise eest välispartnerite ja tarnijate suhtes vastutab andmevalitseja. Kohustused ja õigused tuleks formaliseerida kirjalikus dokumendis. Andmevalitseja peab korralikult tundma partnerite ja tarnijate turbestrateegiat ja regulaarselt veenduma selles, et see strateegia annab teabele rahuldava turvalisuse.

G31 Privaatsus (jätkub)

- Dokumentatsioon. Infosüsteemide kasutamise menetlused ja muu infoturbesse puutuv teave tuleks dokumenteerida. Dokumentatsiooni tuleks talletada vastavalt kohalikele õigusaktidele. Infosüsteemide intsidendilogisid tuleb säilitada vähemalt kolm kuud. Isikuteabe lubatava kasutamise spetsifitseerimiseks tuleks rakendada poliitikat, standardeid ja protseduure.
- Teadvustus- ja koolitusüritused. Neid tuleb rakendada privaatsuspoliitika teatavakstegemiseks töötajaile ja tarnijaile, eriti neile inimestele, kes käsitlevad klientide isikuteavet (st klienditeenindusele).

6 PLAANIMINE

6.1 Eri maade privaatsusseaduste ülevaade. Printsiibid ja peamised erinevused

6.1.1 Enamikus maades on juba kehtestatud oma privaatsusalased õigusnormid. Printsiibid on põhiliselt ühesugused, kuid olulisi erinevusi on isikuandmete määratluses, põhilistes turvameetmetes, mida tuleb rakendada jms. Need erinevused võivad mõjutada IS audiitori rolli, eriti kui ülesanne hõlmab mitut maad ja/või andmehoidlad asuvad teisel territooriumil.

6.1.2 Tabel 1 loetleb üldprintsiibid dokumendist "OECD suunised isikuandmete privaatsuse ja piire ületavate andmevoogude kaitse kohta", mille avaldas Majandusliku Koostöö ja Arengu Organisatsioon (OECD) aastal 1980. ja vaatas läbi aastal 2002.

Tabel 1. ÜLDPRINTSIIBID

Nr.	PRINTSIIP	SELETUS
1	Kogumise piirang	Isikuandmete kogumine on võimalik andmesubjekti (selgekujulisel) nõusolekul ja teadmisel.
2	Andmete kvaliteet	Isikuandmed on asjakohased neil eesmärkidel, milleks neid kasutatakse ning on nende eesmärkide jaoks vajalikus ulatuses täpsed, täielikud ja ajakohased
3	Eesmärgi spetsifitseerimine	Isikuandmete kogumise eesmärgid spetsifitseeritakse hiljemalt andmete kogumise ajaks ning järgnev kasutamine on piiratud nende eesmärkidega või selliste muude eesmärkidega, mis ei ole vastuolus nende eesmärkidega ja on sellised, nagu nad on spetsifitseeritud igal eesmärgi muutumisel.
4	Kasutamise piirang	Isikuandmeid ei tohi avalikustada, teha kättesaadavaiks ega muul viisil kasutada muudel kui ülalspetsifitseeritud eesmärkidel (välja arvatud andmesubjekti või ametivõimude nõusolekul)
5	Turvameetmed	Isikuandmed peaksid olema mõistlike turvameetmetega kaitstud kaotsimineku ning volitamatu juurdepääsu, hävitamise, kasutamise, muutmise, avalikustamise vms riskide eest.
6	Avatus	Isikuandmeid puudutavate arenduste, tavade ja poliitikate kohta peaks kehtima üldine avatuse poliitika. Raskusteta kättesaadavad peaksid olema vahendid, millega teha kindlaks isikuandmete olemasolu ja iseloom, nende kasutamise peamised eesmärgid ning andmevalitseja identiteet ja tavaline asukoht.

G31 Privaatsus (jätkub)

7	Isiku osalus 1	Isikul on õigus saada andmevalitsejalt või muul viisil kinnitust sellele, kas andmevalitsejal on tema kohta andmeid või mitte.
8	Isiku osalus 2	Isikul on õigus olla teavitatud teda puudutavatest andmetest • mõistliku ajaga, • mõõduka tasu (kui seda võetakse) eest, • mõistlikul viisil, • talle kergesti arusaadaval kujul.
9	Isiku osalus 3	Isikul on õigus saada teada, millistel põhjustel talle keeldutakse vastamast päringule, mis vastab printsiipidele 7 ja 8, ning vaidlustada sellist keeldumist.
10	Isiku osalus 4	Isikul on õigus taotleda andmeid enda kohta ning eduka taotluse korral lasta andmeid kustutada, parandada, täiendada või muuta.
11	Isiku osalus 5	Tuleb kehtestada spetsiifilised protseduurid selleks, et isik saaks ettevõttele teatada oma otsuse muutmisest oma isikuteabe kasutamise ja kõrvaldamise kohta ning need muudatused peavad kajastuma kõigis süsteemides ja kõigil platvormidel, kus tema andmeid kasutatakse.
12	Andmevalitseja vastutus	Andmevalitseja vastutab kõigi selliste meetmete järgimise eest, mis viivad ellu ülalloetletud printsiibid.

6.1.3 Ülalmainitud printsiipide põhjal koostatud meelespea tabelis 2 peaks aitama koostada eri maade õigusnormide võrdlusi ning näitab üldjoontes, kuidas neid printsiipe tegelikult rakendatakse. Veerus "PR." on viited printsiipide numbritele tabelis 1.

Tabel 2. MEELESPEA

Nr.	PR.	KÜSIMUSED
1	1	Kas isikuandmete kogumine ükskõik milliseks töötluseks on VÕIMATU, kui selleks puudub isiku ühemõtteline nõusolek või kui see ei toimu isikuga sõlmitud lepingu täitmiseks ega mingitel muudel seadustega selgelt lubatavatel tingimustel? Erandiks on erijuhud, näiteks seoses ühiskonna või riigi turvalisusega; sel juhul koguvad andmeid ametivõimud ning selleks annab volituse muu kui andmeid koguv organ.
2	1	Kas luba isikuandmete kogumiseks ja/või töötlemiseks peab olema igal kolmandal poolel, kellel on vaja neile andmetele juurde pääseda või neid muuta (näiteks väljasttellimise puhul), ning kas ning kas see peab olema andmesubjekti eraldi kirjalik nõusolek lisaks sellele, mille ta annab peaettevõtjale (teiste sõnadega: ükski andmevalitseja ei saa ühelegi kolmandale poolele anda juurdepääsu andmetele ilma andmesubjekti selge ühemõttelise volituseta)?
3	2	Kas andmevalitsejad on kohustatud perioodiliselt kontrollima andmete õigsust ja ajakohastama või kustutama (töötluse käsitlusala seisukohalt) asjassepuutumatu, liigse või aegunud teabe?
4	3	Kas andmevalitsejad on kohustatud tegema andmete kogumise käsitlusala teatavaks andmesubjekti(de)le?
5	3	Kas andmevalitsejad on kohustatud piirama andmete kasutamist nii, et andmeid tohivad kasutada ainult need, kellest teatati andmesubjektidele nende andmete kogumise ajal?
6	3	Kas andmevalitsejad on kohustatud teatama igast andmete kogumise või töötlemise eesmärkide muutumisest andmesubjekti(de)le ja taotlema sellelt/nendelt nõusolekut?
7	4	Kas andmete kasutamisele on piiranguid, mis keelavad igasuguse kasutamise ja avaldamise, milleks ei ole selget volitust andmesubjekti(de)lt?
8	5	Kas on nõudeid minimaalsete turvameetmete kohta, mida andmevalitsejad peavad rakendama lubamatu avaldamise või kasutamise tõrjeks?
9	5	Kas andmevalitsejad peavad koostama turbeplaani ja seda perioodiliselt ajakohastama?
10	5	Kas andmevalitsejad peavad perioodiliselt viima läbi riski kaalutlemise?

G31 Privaatsus (jätkub)

11	5	Kas on mingeid nõudeid, mis teevad iga andmevalitseja organisatsiooni kuuluva isiku üheselt identifitseeritavaks ja subjekti(de) ükskõik milliste andmete poole pöördumise eest vastutavaks?
12	6	Kas andmesubjekti(de)le tuleb tingimata teatada andmevalitseja (isiku või organisatsiooni) identiteet ja kogutavate või töödeldavate andmete iseloom?
13	6	Kas on kasutusel mingid koolitus- või teadvustuskavad personali teavitamiseks isikuteabe kaitse nõuetest?
14	7	Kas andmesubjekt(id) saab/saavad küsida andmevalitsejalt teavet ennast puuduravate andmete olemasolu ja iseloomu kohta?
15	7	Kas andmesubjekti(de)l on võimalik saada andmevalitsejalt enda andmeid ja neid kontrollida?
16	8	Kas vastamiseks küsimustele 15 ja 16 on määratud mingi maksimaalne ajavahemik? Jah, teave tuleks anda mõistlikul viisil ja arusaadaval kujul.
17	9	Kas andmesubjekti(de)l on võimalik vaidlustada kõik andmevalitseja keeldumised teda/neid puudutavate andmete või töötluse olemasolu teatamisest talle/neile?
18	10	Kas andmesubjekti(de)l on võimalik lasta andmevalitsejal kustutada teda/neid puudutavaid andmeid kustutada? Jah.
19	11	Kas andmesubjekt saab igal ajal keelduda ükskõik kellele (ka neile, kes on varem saanud loa) andmast nõusolekut ennast puudutavate andmete kogumiseks?
20	12	Kas on sanktsioone andmevalitsejatele, kes ei järgi ülalloetletud printsiipe?
21	12	Kas on organisatsioone, kelle kohus on kontrollida andmevalitseja vastavust ülalloetletud printsiipidele?

7 AUDITITÖÖ SOORITAMINE

7.1 Organisatsiooni privaatsustavade ja -protseduuride läbivaatamine

7.1.1 IS audiitor peaks hästi tundma auditi plaanimise protsessi. Tuleb koostada auditi kava, mis sisaldab auditi käsitlusala, eesmärke ja ajastust. Auditi kavas tuleks selgelt dokumenteerida aruandluse korraldus.

7.1.2 Tuleks arvestada organisatsiooni ja ta huvipoolte iseloomu ja suurust. Piire (nii sisemaiseid kui ka rahvusvahelisi) ületavate seoste tundmine on tähtis ning aitab määrata auditi käsitlusala ja ajakulu.

7.1.3 IS audiitor peaks õppima tundma organisatsiooni missiooni ja tegevuseesmärke, nende andmete liike, mida organisatsioon kogub ja kasutab, ning organisatsioonile kohaldatavaid õigusnorme, mis võivad sisaldada privaatsusnõudeid. Vaja on tunda ka organisatsiooni struktuuri, sealhulgas olulise personali, kaasa arvatud teabejuhtide ja -omanike, rolle ja kohustusi.

7.1.4 Auditi plaanimise järgu esmane eesmärk on tunda riske, mis ähvardavad organisatsiooni, kui ta ei järgi privaatsust puudutavaid õigusnorme.

7.2 Sooritatavad sammud

7.2.1 IS audiitor peaks sooritama privaatsuse esialgse hindamise, mis aitaks määrata, millist mõju avaldaks organisatsioonile asjakohaste privaatsust puudutavate õigusnormide järgimata jätmine. See aitab määratleda läbivaatuse käsitlusala ning peaks arvestama ka selliseid tegureid nagu kogutava, talletatava ja organisatsioonis mitmesugustel eesmärkidel kasutatava teabe tüüp.

G31 Privaatsus (jätkub)

7.2.2 IS audiitor peaks välja selgitama, kas organisatsioonis on olemas

- privaatsuspoliitika,
- privaatsusametnik,
- andmevalitseja,
- privaatsuskoolituse ja -teadvustuse plaan,
- privaatsuskaebuste käsitluse protsess,
- privaatsusalaste õigusnormide järgimise auditite korraldus,
- privaatsusnõuded väljasttellimisele ja allettevõtjaile.

Kui need on olemas, peaks IS audiitor neid hindama veendumiseks, et nad on kooskõlas kohaldatavate privaatsusalaste õigusaktidega.

7.2.3 IS audiitor peaks viima läbi privaatsuse mõju analüüsi. See tähendab, et tuleb

- tuvastada, analüüsida ja prioriteetida riskid, mis tulenevad sellest, et ei järgita privaatsust puudutavaid õigusnorme;
- tunda mitmesuguseid organisatsioonis hetkel käibivaid privaatsuse mõõte;
- hinnata tugevaid ja nõrku külgi;
- soovitada täiustamise strateegiaid.

7.2.4 IS audiitor peaks koostama aruande, mis dokumenteerib privaatsuse läbivaatuse tulemused. Aruanne peaks visandama eesmärgid ja käsitlusala ning tegema kokkuvõtte sellest, millist tüüpi andmeid ja teavet organisatsioon kogub, talletab ja kasutab.

7.2.5 Aruanne peaks sisaldama teavet organisatsiooni ähvardavate privaatsusega seotud riskide kohta ja kokkuvõtte olemasolevatest riski leevendamise meetmetest või privaatsuse kaitse strateegiatest.

7.2.6 Privaatsuse läbivaatusega avastatud nõrkused, mis tulenevad riski leevendamise meetmete puudumisest või puudulikkusest, tuleks teha teatavaks teabe omanikele ja privaatsuspoliitika eest vastutavatele juhtidele.

7.2.7 Kui privaatsuse läbivaatusega avastatud nõrkusi loetakse olulisteks või kaalukateks, tuleks juhtkonna vastavale tasemele soovitada viivitamatult rakendada parandusmeetmeid.

7.2.8 IS audiitor peaks auditi aruandes esitama sobivad soovitused, pakkudes juhtkonnale võimalusi tugevdada organisatsiooni privaatsusmeetmeid.

G31 Privaatsus (jätkub)

8 ARUANDLUS

8.1 Turvameetmete kontrolli eeskirjad

8.1.1 Kohalikud õigusaktid privaatsuse kohta võivad nõuda mingite turvameetmete olemasolu isikuandmete korraliku kaitse tagamiseks volitamatu juurdepääsu, lubamatu avaldamise, muutmise ja/või kaotsimineku riskide eest.

8.1.2 Järgnev kesksete turvameetmete loetelu aitab saada mõistlikku kinnitust sellele, et kohalikud privaatsusnõuded on täidetud. Tuleb pidada silmas, et kohalikest õigusaktidest võivad tuleneda veel muud meetmed. IS audiitor peaks enne auditi alustamist kontrollima selle tabeli rakendatavust ja täielikkust, nii nagu on määratud jaotise 6.1.3 tabelis 2.

8.2 Infokandjate taaskasutus

8.2.1 Mõistliku kinnituse saamiseks sellele, et isikuandmeid sisaldavaid infokandjaid ja dokumentatsiooni hoiab kogu personal asjakohase hoolikusega, peaks olema käigus formaalne protseduur ja seda tuleks kontrollida.

8.2.2 Enne isikuandmeid sisaldanud infokandja (näiteks elektroonilise, digitaalse või paberkandja) taaskasutust tuleks saada mõistlik kinnitus sellele, et kogu teave on kustutatud. Andmete tundlikkuse või andmekandja iseloomu tõttu tuleb mõnikord hävitada ka infokandja ise.

8.3 Koolitus

8.3.1 Kogu isikuandmeid käsitlevale personalile tuleks plaanida regulaarne turvakoolitus.

8.4 Pääsu reguleerimine

8.4.1 Üldprintsiibina tuleks rakendada teadmisvajaduse põhimõtet (st iga inimene peaks saama juurdepääsu ainult oma töö sooritamiseks vajalikele failidele ja arhiividele).

8.4.2 Pääsuõigused ja kasutajate identifikaatorid tuleks määrata vastavalt sellisele poliitikale.

8.4.3 Kasutaja identifikaatori viivitamatuks ajakohastamiseks või kustutuseks töötaja lahkumise või teisele tööle üleviimise korral peaks olema käigus kirjalik protseduur ja seda tuleks kontrollida.

8.4.4 Personaalarvutite kasutamise kohta peaksid olema korralikud juhendid ja neid tuleks kontrollida. Nad peaksid sisaldama kõiki individuaalse andmeturbe aspekte, näiteks andmete regulaarse varundamise vajadust, seda, et tööarvuteid ei tohiks jätta järelevalveta jms.

8.4.5 Sisemine võrk tuleks adekvaatselt kaitsta turbevahenditega, näiteks tulemüüridega.

8.4.6 Tuleks kontrollida ootamatuste käsitluse plaani, mille eesmärk on taastada isikuandmete arhiivid ettemääratud ajaga.

8.5 Hooldus ja tugi

8.5.1 Iga hoolduse ja toe otstarbeline juurdepääs tuleks logida ja seirata.

8.6 Andmeterviklus

8.6.1 Tuleks saada mõistlik kinnitus sellele, et igas tööarvutis on installeeritud viirusetõrjetarkvara ja seda ajakohastatakse regulaarselt, aboneerides seda valitud viirusetõrjefirmalt.

8.6.2 Regulaarselt tuleks kontrollida, kas operatsioonisüsteemi ja igasuguse rakendatava tarkvara tarnijail on uusi paiku või täiendusi.

8.6.3 Plaaniline andmete varundamine serveritel, suurarvutitel ja personaalarvutitel peaks olema regulaarne.

8.7 Ruumidesse pääsu reguleerimine

8.7.1 Kõik organisatsiooni ruumidesse sisenejad tuleks registreerida. Väljaspool tööaega tööle tulevad töötajad peaksid andma allkirja registreerimisraamatusse.

8.8 Riskianalüüs

8.8.1 Riskianalüüs eesmärgiga tuvastada isikuandmete riskid ja turvaaugud tuleks sooritada regulaarselt.

9 JÕUSTUMISKUUPÄEV

9.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. juunil 2005 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

G31 Privaatsus (jätkub)

LISA

Allikaviited

AICPA/CICA privaatsuse raamstruktuur. Ameerika Sertifitseeritud Audiitorite Instituut (AICPA) ja Kanada Sertifitseeritud Audiitorite Instituut (CICA). 2003.

Privaatsus. Riski kaalutlemine. Siseaudiitorite Instituudi (IIA) teadusfond. Aprill 2003.

OECD suunised isikuandmete privaatsuse ja piire ületavate andmevoogude kaitse kohta. Majandusliku Koostöö ja Arengu Organisatsioon (OECD). 1980, 2002.

Isikuandmete arvutifailide reguleerimise suunised. ÜRO Inimõiguste Ülemkomissari Amet. 1990.

Ettevõtetevahelise e-kaubanduse turvalisuse, privaatsuse ja teenuse rahvusvaheline standard. Rahvusvaheliste Standardite Akrediteerimiskogu (ISAB). IES 2000 (B2B). 2000.

Ettevõtte ja tarbija vahelise e-kaubanduse turvalisuse, privaatsuse ja teenuse rahvusvaheline standard. Rahvusvaheliste Standardite Akrediteerimiskogu (ISAB). IES 2000 (B2C). 2000.

Programmi Safe Harbor privaatsuspõhimõtted. USA Kaubandusministeerium. 21. juuli 2000.

USA Kaubandusministeeriumi programm "Safe Harbor". USA Kaubandusministeerium. *www.export.gov/safeharbor*

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Auditi tööd sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.2 Seos COBITiga

1.2.1 Lai juhtimiseesmärk TT4 "Tagada pidev teenus" määrab: "Pideva teenuse tagamise IT-protsessi tuleb juhtida nii, et täidetaks talitlusnõue teha IT-teenused vastavalt vajadustele kättesaadavaiks ning tagada suurema katkestuse korral minimaalne toime talitlusele.

1.3 Toetumine COBITile

1.3.1 Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ning COBITi juhtimiseesmärkide ja nendega seotud juhtimistavade arvestamisel. JSP läbivaatusel IT seisukohalt on kõige asjakohasematena valitavad ja kohaldatavad COBITi protsessid alljärgnevas loetelus jagatud esmasteks ja teisesteks. Protsessid ja juhtimiseesmärgid, mis tuleb valida, võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest.

1.3.2 Esmajärjekorras

- PO9 – Hinnata IT riskid ja hallata neid
- HE6 – Hallata muutusi
- TT1 – Määratleda teenusetasemed ja hallata neid
- TT4 – Tagada pidev teenus
- TT10 – Hallata probleeme
- TT11 – Hallata andmeid
- TT12 – Hallata füüsilist keskkonda
- TT13 – Hallata käitust

1.3.3 Teises järjekorras

- PO4 – Määratleda IT protsessid, organisatsioon ja seosed
- S3 – Tagada vastavus välisnõuetele (COBIT v3)
- PO7 – Hallata IT inimressursse
- HE5 – Hankida IT-ressursid

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

- TT2 – Hallata kolmandate osapoolte teenuseid
- TT5 – Tagada süsteemide turvalisus
- TT9 – Hallata konfiguratsiooni
- SH1 – Seirata ja hinnata IT töötulemusi

1.3.4 JSP läbivaatuse jaoks kõige asjakohasemad teabekriteeriumid on

- esmajärjekorras: toimivus, tõhusus, käideldavus ja vastavus;
- teises järjekorras: konfidentsiaalsus, terviklus ja usaldatavus.

1.4 Suunise eesmärk

1.4.1 Tänapäeva läbipõimunud majanduses on organisatsioonid nende tegevust katkestavate tehniliste raskuste võimaluste suhtes tundlikumad kui eales varem. Talitluse jaoks elutähtsa teabe käideldavust, terviklust ja konfidentsiaalsust võib mõjutada iga hädaolukord, alates üleujutustest või põlengust ning lõpetades viiruste ja küberterrorismiga.

1.4.2 JSP esmane eesmärk on hallata organisatsiooni riske, mis tulenevad juhtumist, et organisatsiooni talitlus ja/või infosüsteemide teenused on täielikult või osaliselt rivist väljas, ning aidata organisatsioonil toibuda selliste sündmuste toimest.

1.4.3 Selle suunise eesmärk on kirjeldada soovitatavaid tavasid jätkusuutlikkuse plaani (JSP) läbivaatuseks IT seisukohalt.

1.4.4 Selle suunise eesmärk on asjakohaste esmaste ja teiseste juhtimiseesmärkide saavutamiseks tuvastada, dokumenteerida, kontrollida ja hinnata IT seisukohalt organisatsioonis rakendatavad JSP protsessiga seotud meetmed ja nendega kaasnevad riskid.

1.4.5 See suunis annab juhiseid IS auditeerimise standardi S6 "Audititöö sooritamine" rakendamiseks nii, et jätkusuutlikkuse plaani läbivaatusel IT seisukohalt saadaks piisavaid, usaldatavaid, asjassepuutuvaid ja kasulikke auditi asitõendeid. IS audiitor peaks seda arvestama otsustamisel, kuidas saavutada ülalnimetatud standardi elluviimine, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama iga lahknevust.

1.5 Suunise rakendamine

1.5.1 Seda suunist rakendatakse organisatsioonis JSP läbivaatusel IT seisukohalt.

1.5.2 Selle suunise rakendamisel peaks IS audiitor arvestama ta juhiseid seotult muude asjassepuutuvate ISACA standardite ja suunistega.

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

1.6 Terminoloogia

1.6.1 Suurtähtlühendid

- Jätkusuutlikkuse plaan (JSP)
- Talitlusliku toime analüüs (TTA)
- Avariijärgse taaste plaan (ATP)

1.6.2 Jätkusuutlikkuse plaanimine on protsess, millega töötatakse välja ennetavad ettevalmistused ja protseduurid, mis võimaldavad organisatsioonil reageerida katkestusele nii, et plaaniliste katkestustasemete või olulise muudatuse korral säilivad elutähtsad talitlusfunktsioonid. Lihtsamalt öeldes, JSP on akt, millega ennetavalt strategiseeritakse meetod hädaolukorra vältimiseks, kui see on võimalik, ja ta tagajärgede haldamiseks, piirates tagajärgi sellise ulatuseni, et talitlus suudab nende toime summutada.

1.6.3 JSP tähendab täielikku jätkusuutlikkuse plaanimise protsessi, ta sisaldab muuhulgas talitluslikke, tehnoloogilisi, inim- ja regulatiivseid aspekte.

1.6.4 JSP määratleb rollid ja kohustused ning piiritleb talitlusliku toime analüüsil põhinevad elutähtsad infotehnoloogia rakendusprogrammid, operatsioonisüsteemid, võrgud, töötajad, rajatised, andmefailid, seadmed ja ajastused. JSP on kõikehõlmav otsustus järjekindlate meetmete kohta, mida tuleb rakendada enne hädaolukorda, selle ajal ja pärast seda. Ideaaljuhul võimaldab JSP ettevõttel jätkata katkestuse korral tegevust ning elada üle avariilised katkestused elutähtsates infosüsteemides.

1.6.5 Talitlusliku toime analüüs sisaldab elutähtsate talitlusfunktsioonide ja töövoo piiritlemist, selgitab välja katkestuse kvalitatiivse ja kvantitatiivse toime ning seab prioriteedid taasteaja-alastele eesmärkidele (TAE-dele).

1.6.6 ATP on JSP keskne komponent ja kujutab endast JSP tehnoloogilist aspekti – ennetavat plaanimist ja ettevalmistusi, mis on vajalikud kahju minimeerimiseks ja elutähtsate talitlusfunktsioonide säilimist hädaolukorras. ATP koosneb järjekindlatest meetmetest, mida tuleb rakendada enne hädaolukorda, selle ajal ja pärast seda. Mõistlik ATP koostatakse igakülgse plaanimise protsessiga, mis hõlmab ettevõtte kõiki talitlusprotsesse. Avariijärgse taaste strateegiate hulka kuuluvad alternatiivsete asukohtade (kuum-, soe- ja külmvaruna) kasutamine, varu-arvutuskeskused, vastastikused lepped, sidekanalid, õnnetuskindlustus, talitlusliku toime analüüsid ja õiguslik vastutus.

2 JSP ÜLEVAADE IT SEISUKOHALT

2.1 JSP komponendid IT seisukohalt

2.1.1 JSP IT-komponent määratleb reageerimise ja taaste protsessi, mis tagab IT töö käideldavuse ning talitlusprotsessi toetamiseks elutähtsate protseduuride, rakenduste, operatsioonide, süsteemide, andmesalvestite, võrkude ja rajatiste taasintegratsiooni.

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

2.1.2 JSP komponentide hulka kuuluvad alljärgnevad.

- Tuvastamine: tuvastada potentsiaalsed ohud ja riskid talitlusele.
- Vältimine: vältida intsidenti või minimeerida ta tõenäosust.
- Avastamine: piiritleda tingimused, mille korral organisatsioon otsustab siirduda ootamatuse olekusse.
- Väljakuulutamine: spetsifitseerida tingimused, mille korral kuulutatakse välja ootamatus ja määrata isik(ud), kes võib/võivad selle välja kuulutada.
- Eskaleerimine: spetsifitseerida tingimused, mille korral ootamatus eskaleeritakse, ning määrata ootamatuse eskaleerimise kord ja selles osalev(ad) isik(ud).
- Piiramine: spetsifitseerida viivitamatud meetmed, mida on vaja rakendada intsidendi mõju piiramiseks või minimeerimiseks klientidele, tarnijaile, teenuseandjaile, huvipooltele, töötajaile, varadele, suhtekorraldusele ja talitlusprotsessile.
- Teostamine: spetsifitseerida täielik loetelu meetmetest, mida tuleb järgida ootamatuse oleku väljakuulutamiseks (näiteks töötlus väljaspool alalist asukohta, taaste varukoopiaga, andmekandjad ja teatmikud väljaspool alalist asukohta, töötajate transportimine ning lepingud turustajate ja tarnijatega).

Taaste: taaste tähendab etteplaanimist ja ettevalmistusi, mis on vajalikud hädaolukorra kahjuliku talitlusliku toime (näiteks rahalise kahju ja mainekahjustuse) minimeerimiseks, kiirema toibumise soodustamiseks ja organisatsiooni elutähtsaid talitlusfunktsioone toetavate kesksete tehnoloogiliste varade kestvuse tagamiseks, aktsepteeritava ajaga. Kesksed aspektid, mis tuleb läbi vaadata, on järgmised.

- Jätkamine: elutähtsate ja ajatundlike protsesside jätkamine kohe pärast katkestust ja enne deklareeritud keskmise tõrketu töövältuse (MTBF) lõppu.
- Elustamine: oluliste ja vähem ajatundlike protsesside elustamine on seotud elutähtsate protsesside jätkamisega.
- Ennistamine: tegutsemiskoha remont ja ennistamine algsesse olekusse ning talitluse jätkamine tervikuna või täiesti uue tegutsemiskoha kasutuselevõtt.
- Kolimine: kolimine alternatiivsesse asukohta ajutiseks või alaliseks, sõltuvalt katkestusest. Igat liiki katkestuste puhul ei tarvitse kolimine olla vajalik.

Kriisihaldus: organisatsiooni kriisireaktsiooni üldine toimiv ja õigeaegne koordineerimine eesmärgiga vältida organisatsiooni kasumlikkuse, maine või tegutsemisvõime kahjustamist või minimeerida seda.

2.2 JSP elemendid

2.2.1 JSP üks oluline element on riski kaalutlemine, mille käigus tuleb tuvastada ja analüüsida potentsiaalsed nõrkused ja ohud ning nende allikad. Riski kaalutlemine kujutab endast protsessi, millega tuvastatakse organisatsiooni potentsiaalsed riskid,

hinnatakse elutähtsad funktsioonid, mis on organisatsioonile vajalikud tegevuse jätkamiseks, määratletakse meetmed riskile avatuse vähendamiseks ja hinnatakse selliste meetmete maksumus. Riskihüvede analüüs on riski kaalutlemise tulem, mis detailiseerib potentsiaalsed ohud ja nendega seotud turvaaugud koos vajalike ootamatus- ja leevendusmeetmetega ning lõpeb riskide katmisest tulenevate hüvede kirjeldamisega.

2.2.2 Talitluse katkemisest tulenevate üldiste rahaliste nõrkuste ja tegutsemismõjude hindamiseks tuleks riski kaalutlemise järel sooritada TTA. TTA peaks välja selgitama IS infrastruktuuriga toetatavad elutähtsad talitlusprotsessid ja aitama neile määrata prioriteete; muuhulgas peaks ta sisaldama meetmete tasuvuse analüüsi mitmesugustes katkestuste stsenaariumides.

2.3 JSP kesksed tegurid

2.3.1 JSP peab

- olema arusaadav ning raskusteta kasutatav ja hooldatav;
- andma juhtkonnale igakülgse ettekujutuse süsteemide normaalse töö katkemise mõjudest talitlusele ning toimiva JSP koostamiseks ja hoolduseks vajalikust kogupanusest;
- saavutama täitevjuhtide kohustumuse toetada seda panust ja osaleda selles;
- piiritlema elutähtsad teaberessursid, mis on seotud talitluse tuumprotsessidega;
- piiritlema meetodid andmete konfidentsiaalsuse ja tervikluse säilitamiseks;
- hindama iga talitlusprotsessi ta elutähtsuse määramiseks. Elutähtsuse tunnused on näiteks järgmised:
  - protsess toetab inimeste tervist ja ohutust,
  - protsess on vajalik õigusaktide või põhikirja nõuete täitmiseks,
  - protsessi katkestamine mõjutab tulu,
  - võib mõjutada tegevusalast mainet, ka klientide hulgas;
- keskendama plaani tähelepanu
  - avariihaldusele,
  - avarii toime minimeerimisele juhul, kui avarii ei ole hallatav,
  - korrakohasele taastele,
  - tegevuse ja kesksete teenuste pidevusele;
- valideerima mitmesuguste süsteemide taasteaja-alased eesmärgid (TAE-d) ja taastepunktide-alased eesmärgid (TPE-d) ja nende vastavus talitluse eesmärkidele;
- piiritlema tingimused, mis aktiveerivad ootamatuste käsitlemise plaani;

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

- määrama, millised ressursid on ootamatuse järgus olemas ning millises järjestuses nad taastatakse;
- määrama taasteks vajalikud võimaldajad (inimesed ja ressursid);
- valima projektirühmad vastavalt tehnoloogilistele ja talitluslikele keskkondadele, nii et plaani koostamiseks oleksid mõistlikult esindatud kesksed ja elutähtsad talitlusliinid;
- määrama võimaldajate, tugipersonali ja töötajate vahelise suhtluse meetodid;
- piiritlema talitluse taastega seotud geograafilised tingimused;
- määratlema taastenõuded talitlusfunktsioonide seisukohalt;
- määratlema, kuidas tuleb JSP kaalutlused integreerida talitluse pideva plaanimise ja süsteemiarenduse protsessidega, nii et plaan jääks elujõuliseks pikema aja kestel;
- tegema teoks protsessi JSP pideva sobivuse perioodiliseks läbivaatuseks ning dokumendi õigeaegseks ajakohastuseks, eriti, kui on muutusi tehnoloogias ja protsessides või õiguslikes või talitluslikes nõuetes. JSP strateegiaid võidakse muuta ka riski kaalutlemiste ja nõrkuste hindamiste tulemuste põhjal;
- töötama välja JSP igakülgse testimise metoodika, mis hõlmab juhtimise, talitluse ja tehnilise külje testimist;
- tegema teoks muutuste halduse protsessi ning hooldatavust soodustavad sobivad versioonihalduse meetmed;
- määrama mehhanismid ja otsustajad taasteprioriteetide muutmiseks algsetest plaanilistest suuremate või väiksemate ressursside tõttu;
- dokumenteerima formaalsed koolituse metoodikad.

3 SÕLTUMATUS

3.1 Kutsealane sõltumatus

3.1.1 Kui IS audiitor, kellele on antud auditeerimisülesanne, on organisatsioonis varem osalenud JSP-ga seotud suvalise protsessi kavandamises, väljatöötamises, evitamises või hoolduses, võib see kahjustada ta sõltumatust. Igasuguse võimaliku huvide vastuolu puhul tuleks sellest selgelt teatada organisatsioonile ja enne ülesande vastuvõtmist tuleks organisatsioonilt saada kirjalik nõusolek. Selliste olukordade käsitlemiseks peaks IS audiitor toetuma asjakohastele suunistele.

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

4 PÄDEVUS

4.1 Oskused ja teadmised

4.1.1 IS audiitor peaks andma mõistliku kinnituse selle kohta, et tal on JSP ja selle komponentide läbivaatuseks vajalikud teadmised ja oskused.

4.1.2 IS audiitor peaks olema pädev otsustama, kas JSP on organisatsiooni vajadustega kooskõlas.

4.1.3 IS audiitoril peaksid olema adekvaatsed teadmised JSP-ga seotud aspektide läbivaatuseks. Kui on vaja teavet asjatundjatelt, tuleks seda hankida välistest kutsealastest allikatest. Väliste asjatundjaressursside kasutamise faktist tuleks kirjalikult teatada organisatsioonile.

4.1.4 JSP läbivaatus on olemuselt ettevõttespetsiifiline ning et läbivaatus oleks toimiv, peab IS audiitor seda alustades saama üldise ettekujutuse tegevuskeskkonnast, sealhulgas tehes endale selgeks organisatsiooni missiooni, organisatsioonile omased põhikirja või õigusnormide nõuded, tegevuseesmärgid, asjassepuutuvad talitlusprotsessid, nende protsesside teabevajadused, IS strateegilise väärtuse ja selle kooskõla ettevõtte või organisatsiooni üldise strateegiaga.

4.1.5 IS audiitor peaks JSP või poliitikate ning testimis- ja taasteplaanide koostamise võtma käsile ainult siis, kui tal on vajalikud teadmised, pädevus, oskused ja ressursid. Selliste olukordade käsitlemiseks peaks IS audiitor toetuma asjakohastele suunistele.

5 PLAANIMINE

5.1 Läbivaatuse käsitlusala ja eesmärgid

5.1.1 Vajadusel organisatsiooniga nõu pidades peaks IS audiitor selgelt määratlema JSP läbivaatuse käsitlusala ja eesmärgid. Aspektid, mis tuleb läbivaatusega katta, tuleks selgelt sõnastada käsitlusala ühe osana.

5.1.2 Tuleks määratleda ja organisatsiooniga kokku leppida ka lahenduse huvipooled läbivaatuse seisukohalt ja aruande saajad.

5.2 Metoodika

5.2.1 IS audiitor peaks sõnastama auditi metoodika nii, et läbivaatuse käsitlusala ja eesmärke saaks saavutada objektiivsel ja professionaalsel viisil.

5.2.2 Auditi metoodika sõltub JSP järgust organisatsioonis.

5.2.3 Metoodika peaks arvestama, et JSP läbivaatus on rühmatöö, mis hõlmab aktiivseid ja püsivaid liikmeid ja ka arutamisi kasutajarühmadega.

5.2.4 Metoodika tuleks asjakohaselt dokumenteerida ja ta peaks vajaduse korral määrama välise asjatundjateabe vajadused.

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

5.2.5 Olulised alad, näiteks prioriteetide seadmine talitlusprotsessidele ja tehnoloogiatele ning riski kaalutlemise tulemused, peaksid andma mõistliku kinnituse sellele, et plaan on toimivalt ja nõuetekohaselt tehtud teoks.

5.2.6 Kui see on organisatsioonis tavaks, tuleb IS audiitoril võib-olla saada JSP auditi plaani ja metoodika kohta saada organisatsioonilt nõusolek.

6 JSP LÄBIVAATUSE SOORITAMINE IT SEISUKOHALT

6.1 Sooritamine

6.1.1 Läbivaadatavad aspektid ja läbivaatuse protsess tuleks otsustada võttes arvesse kavatsetavat läbivaatuse käsitlusala ja eesmärki ning plaanimisprotsessi osana määratletud metoodikat.

6.1.2 Üldiselt tuleks andmete kogumisel, analüüsimisel ja tõlgendamisel asjakohaselt uurida kasutadaolevat dokumentatsiooni (näiteks JSP-d, ATP-d, TTA-d, tegevusriski analüüsi ja ettevõtte riskihalduse raamstruktuuri). Kogu see teave ei tarvitse olla kergesti kättesaadav, kuid peab olema vähemalt elementaarne riskikaalutluslik analüüs, mis määratleb elutähtsad talitlusprotsessid koos IT-põhiste riskidega.

6.1.3 Peamised JSP riskialad peaksid hõlmama varem avastatud JSP nõrkusi ja pärast viimast JSP testimist tehtud muudatusi süsteemide keskkonnas (rakendustes, seadmetes, sides, protsessides, personalis jm).

6.1.4 Kõigi seni märkamata jäänud ja võib-olla järelkäsitlust vajavate JSP probleemide väljaselgitamiseks tuleks IS audiitoril läbi vaadata järgmised dokumendid:

- intsidendiaruanded,
- eelmiste uurimiste aruanded,
- järeltoimingud,
- auditite töödokumendid eelmistest uurimistest,
- sise- ja välisauditite aruanded,
- sisemiste testide aruanded ja parandusmeetmete plaan,
- avaldatud valdkonnateave ja allikad.

6.1.5 Süsteemide keskkonna muutuste väljaselgitamiseks peaks IS audiitor vestlema organisatsiooni personaliga ja teenuseandjatega ning analüüsima kulukirjeid ja -aruandeid, vaatama üle IT-ruumid, vaatama läbi riistvara ja tarkvara inventariloetelud ja analüüsima asjakohaseid andmeid spetsialiseeritud tarkvaraga.

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

6.1.6 IS audiitoril tuleks läbivaatusel võtta arvesse kõik testimise järgud:

- testimiseelne: rida toiminguid tegeliku testimise ettevalmistuseks;
- test: tegelik JSP testimise toiming;
- testimisjärgne: rühma tegevuste lõpetustoimingud;
- käivitusjärgne läbivaatus: plaani tegelikule käivitusele järgnevate toimingute läbivaatus.

6.1.7 Testimisplaani eesmärgid tuleks läbi vaadata, kontrollides, kas testimisplaan taotleb järgmist:

- kontrollib JSP täielikkust ja täpsust;
- hindab JSP-ga seotud personali sooritust;
- hindab töörühmade koolitust ja teadlikkust;
- hindab koordineerimist JSP-rühmade, ATP-rühmade, väliste tarnijate ja teenuseandjate vahel;
- mõõdab varuasukoha võimet ja suutvust rahuldada organisatsiooni nõudeid;
- hindab elutähtsate andmike võtu võimet;
- hindab varuasukohta ümber paigutatud seadmete ja materjalide seisundit ja kogust;
- mõõdab organisatsiooni käitus- ja töötlustegevuse üldist sooritust.

6.1.8 JSP testimine tuleks kavandada hoolikalt, vältides talitlusprotsesside häirimist. JSP testimise teatavad alad tuleks piiritleda iga-aastase riskiläbivaatuse osana, tuleks vältides selle töö dubleerimist. JSP testimisplaani läbivaatamisel peaks IS audiitor kontrollima järgmist:

- testimisplaani käsitlusala ja eesmärgid;
- testimisplaani sagedus, metoodika ja läbivaatused;
- testide tüüp, sobivus ja piisavus;
- rakendused;
- andmete maht;
- talitlusalad;
- võrgu ümbermarsruutimine;
- süsteemide turvaaugud, läbitung ja reageerimine sissetungile ja intsidentidele;
- muutuse-, konfiguratsiooni- ja paigahaldus;
- auditi asitõendite kriteeriumid ja nõuded asitõenditele;

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

- testkeskkond esindab töökeskkonda ja erandid on dokumenteeritud;
- testimise toimivus ning selle seos riski kaalutlemise ja talitlusliku toime hindamise järeldustega.

6.1.9 Sündmusejärgse olukorra stsenaariumi läbivaatamisel tuleks IS audiitoril kontrollida järgnev:

- katkestuse põhjus ja iseloom;
- personali, infrastruktuuri ja seadmete kahjustuse ulatus;
- toime tõsidus;
- käimasolevad leevendamisharjutused;
- mõjutatud teenused;
- kahjustatud andmikud;
- objektid, mida saab päästa;
- objektid, mida saab parandada, ennistada ja/või asendada;
- kindlustusnõuded;
- mõjutatud protsessid;
- IT-protsessi taastamiseks kuluv aeg;
- tegevusplaan, taasterühmad, rollid ja kohustused.

6.1.10 Järeldused ja soovitused peaksid põhinema andmete objektiivsel analüüsil ja tõlgendamisel.

6.1.11 Kogutud andmete, sooritatud analüüsi, tehtud järelduste ja soovitatavate parandusmeetmete kohta tuleks säilitada sobivad kontrolljäljed.

6.1.12 Enne aruande viimistlust tuleks vajaduse korral saada leidude ja soovituste kohta saada kinnitus organisatsioonilt.

6.2 Läbivaadatavad aspektid

6.2.1 Tavaliselt peaks JSP käsitlema järgmisi keskseid küsimusi.

- Miks tuleks seda teha?
- Kuidas tuleks seda teha?
- Kellel on vaja seda teha?
- Mis tuleb teha?
- Millal seda tuleks teha?
- Kus tuleks seda teha?
- Milliste poliitikate, eeskirjade ja standardite järgi tuleks seda teha?

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

- Kes saab plaani muuta ja millistel asjaoludel?
- Millistel tingimustel kuulutatakse hädaolukord lõppenuks?

6.2.2 Tuleks läbi vaadata organisatsioonilised aspektid veendumiseks järgnevas.

- JSP on kooskõlas organisatsiooni üldise missiooni, strateegiliste sihtidega ja tegevusplaanidega.
- JSP-d ajakohastatakse süstemaatiliselt ja teda võib pidada ajakohaseks.
- JSP-d testitakse, vaadatakse läbi ja kontrollitakse ta jätkuva sobivuse otsustamiseks perioodiliselt.
- JSP testimiseks, elluviimiseks ja hoolduseks tehakse eraldisi eelarvest.
- Riskianalüüse korraldatakse reeglipäraselt.
- IT ja side inventariloendite regulaarseks ajakohastuseks on kasutusel formaalne protseduur.
- Organisatsiooni juhtkonnal ja personalil on JSP rakendamiseks vajalikud oskused ja kasutusel on sobiv koolituskava.
- Ootamatuse puhuks on olemas meetmed asjakohase reguleerimiskeskkonna (näiteks kohustuste lahususe ning andmetele ja infokandjatele juurdepääsu reguleerimise) säilitamiseks.
- Võimaldajad on piiritletud ning isikute rollid ja kohustused on adekvaatselt määratletud, avaldatud ja teatavaks tehtud. Tavaliselt moodustatakse tuumrühmad, näiteks avariitoimingute rühm, kahjustuste hindamise rühm ja avariihalduse rühm. Neid tuumrühmi toetavad asukohavälise talletuse rühm, tarkvararühm, rakenduste rühm ja turvarühm. On avariitalitluse rühm, võrgu taaste rühm, siderühm, transpordirühm, kasutajariistvara rühm, andmevalmenduse ja -salvestuse rühm, haldustoe rühm, materjalide rühm, päästerühm ja kolimisrühm.
- Sidekanalid on täielikult dokumenteeritud ja organisatsioonis avaldatud.
- Organisatsiooni allüksuste vaheline liidestus ja selle toime on arusaadav.
- Väliste teenuseandjate rollid ja kohustused on määratud, dokumenteeritud ja teatavaks tehtud.
- Väliste teenuseandjate ja klientidega koordineerimise protseduurid on dokumenteeritud ja teatavaks tehtud.
- JSP-rühmad on mitmesuguste JSP ülesannete jaoks määratud, selgelt on kehtestatud rollid ja kohustused ning aruandlus juhtkonnale, mis määratleb jälgitavuse.
- Säilitatakse vastavus põhikirja ja õigusaktide nõuetele.

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

6.2.3 Tuleks läbi vaadata plaanimise aspektid veendumiseks järgnevas.

- Kesksete talitlusprotsesside analüüsi ühe osana on kasutusel metoodika, millega määrata iga protsessi moodustavad tegevused.
- Plaanitud IS tehnoloogia arhitektuur JSP jaoks on kõlblik ning juhul, kui talitluse katkemine mõjutab keskseid IT-protsesse, annab tulemuseks ohutu ja turvalise käituse.
- Enne JSP rakendamist sooritati riski kaalutlemine ja TTA.
- TTA hõlmab riskide muutusi ja vastavat mõju JSP-le.
- TTA selgitab välja elutähtsate talitlusprotsesside taastamise olulised ajapiirid.
- Riske vaadatakse läbi perioodiliselt.
- Ootamatutest sisemistest või välistest sündmustest tekkivate probleemide halduseks, eraldamiseks ja minimeerimiseks on kasutusel asjakohased intsidentidele reageerimise plaanid.
- JSP testimiseks ja hoolduseks on olemas sobiv ajakava.
- Tuleks sooritada kohapealne test, simuleerides sündmuste ja nende võimalike tagajärgede vallandamist.
- On olemas JSP elutsükkel ning seda järgitakse väljatöötuse, hoolduse ja uuendamise ajal.
- JSP vaadatakse läbi perioodiliste vaheaegadega, et veenduda ta jätkuvas sobivuses organisatsioonile.

6.2.4 Tuleks läbi vaadata protseduurilised aspektid veendumiseks järgnevas.

- Tippjuhtkond on JSP rakendamisel tõsine tõukejõud.
- Kõrgeim prioriteet on antud töötajate ja elutähtsate ressursside ohutusele.
- Ressurssidele ja nende taastamisele on antud prioriteedid ja need on taasterühmadele teatavaks tehtud.
- Kogu organisatsioonis luuakse teadlikkus avarii toimest talitlusele.
- Adekvaatsed hädaolukorrale reageerimise protseduurid on olemas ja testitud.
- Avariijärgses hindamises ja taastes osalejad on kogu organisatsioonis selgelt määratud ning rollid ja kohustused on detailselt kirjeldatud.
- Viiakse läbi vajalikul tasemel koolitusi, sealhulgas simulatsioontestimisega õppusi.
- Evakuatsiooniplaanid on olemas ja neid testitakse perioodiliselt.
- Varu-inimressursid on määratud ja on olemas.
- Mobiiltelefoni vms sidevahendi helistuspuid vaadatakse läbi, testitakse ja ajakohastatakse regulaarselt.

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

- Alternatiivside strateegiad on piiritletud.
- Varunduse ja taaste protseduurid on JSP osa.
- Varukoopiad on kättesaadavad.
- Kasutusel on sobiv varunduse rotatsiooni tava.
- Väliste varuasukohtade (kuum-, soe- või külmvaru) käideldavust ja usaldatavust testitakse.
- Säilitatakse asjakohaseid asukohaväliseid andmikke.
- Säilitatakse andmete ja teabe konfidentsiaalsus ja terviklus.
- Asjakohastel juhtudel on olemas meediaga suhtlemise strateegiad.
- JSP-d testitakse regulaarselt ja testimise tulemused dokumenteeritakse.
- Testimise tulemuste põhjal algatatakse parandusmeetmed.

On olemas adekvaatne kaitse kindlustusega.

6.3 Infoteenuste väljasttellimine

6.3.1 Igasugune negatiivne toime teenuseandja tegevusele või tema talitluse katkemine mõjutab otseselt organisatsiooni ja ta kliente. Kui organisatsioon on oma IS-tegevused, mis mõjutavad JSP-protsessi, täielikult või osaliselt delegeerinud välisele selliste teenuste andjale (teenuseandjale), peaks IS audiitor kontrollima, kas teenuseandja JSP-protsess vastab organisatsiooni JSP-le ning kas teenuse kasutajal on olemas dokumenteeritud lepingud, kokkulepped ja eeskirjad.

6.3.2 Selline läbivaatus peaks ka kontrollima, kas lepe väljasttellitava teenuse andjaga sisaldab infosüsteemiteenuste ja -toodete pakkumusega kaasneva vahendite, meetodite, protsesside ja struktuuri ning kvaliteediohje kirjeldust.

6.3.3 IS audiitor peaks õppima tundma väljasttellitavate teenuste iseloomu, ajastust ja ulatust. IS audiitor peaks välja selgitama, milliseid meetmeid rakendab teenuse tarbija organisatsiooni jätkusuutlikkuse talitlusnõude rahuldamiseks, teenuseandjast partneri JSP-d arvestades. Väljasttellitava tegevuse läbivaatamisel peaks lisaks kõigile ülalnimetatud auditinõuetele võtma arvesse järgneva.

- Kas lepe tagab takistuste ja kitsendusteta õigused auditeerida teenuseandjat, kui organisatsioon peab seda vajalikuks?
- Kas lepe pakub organisatsioonile adekvaatset kaitset teenuseandja talitluse katkemise puhul?
- Kas lepe tagab avarii korral teenuste pidevuse?
- Teenuseandja käsutuses olevate organisatsiooni andmete terviklus, konfidentsiaalsus ja käideldavus.

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

- Organisatsiooni personali rahulolematus väljasttellimise korraldusega või lojaalsusetus väljasttellimise tõttu.
- Pääsu reguleerimine ja turbehaldus teenuseandja territooriumil.
- Rikkumistest teatamine ja järeltoimingud teenuseandja poolel.

Võrguturbe meetmed, muudatuste ohje ja testimine teenuseandja territooriumil.

7 ARUANDLUS

7.1 Aruande sisu

7.1.1 IS audiitor peaks koostama aruandeid JSP-ga hõlmatud protsesside, rajatiste ja tehnoloogiate kohta, eeldatud riskide kohta ja selle kohta, kuidas neid riske käsitletakse ootamatuse korral. Keskne edutegur on läbivaatuse soorituse seire. JSP läbivaatuse tulemusena koostatud aruandes tuleksid esitada järgmised aspektid.

- Käsitlusala, eesmärk, kaetav periood, järgitud metoodika ja eeldused.
- Lahenduse üldine hinnang, väljendatuna kesksete tugevate ja nõrkade kohtade kaudu, koos nõrkuste tõenäoliste mõjudega.
- Soovitused oluliste nõrkuste ületuseks ja lahenduse täiustuseks.
- Asjassepuutuvatele COBITi juhtimiseesmärkidele, nendega seotud juhtimistavadele ja COBITi teabekriteeriumidele vastavuse ulatus ning iga lahknevuse toime.
- Mõistlik kinnitus sellele, et JSP protsess ja asjakohased sisemised meetmed tagavad võimaluse katkestuse korral taastada IT-süsteemid vastuvõetava ajaga. Aruanne peaks esitama järeldused, soovitused ja võimalikud reservatsioonid.
- Soovitused selle kohta, kuidas saaks saadud kogemust kasutada analoogiliste tulevaste lahenduste või ettevõtmiste täiustamiseks.
- Muud teemad, sõltuvalt ülesande käsitlusalast.

7.1.2 Aruanne tuleks esitada juhtkonna vastavale tasemele ja auditikomisjonile, kui see on loodud.

7.2 Nõrkused

7.2.1 JSP läbivaatusel avastatud nõrkused, mis on tingitud turvameetmete puudumisest, nende halvast rakendamisest või nõrkustega kaasnevate riskide vastuvõetava tasemeni vähendamata jätmisest, tuleks teha teatavaks talitlusprotsessi omanikule ja JSP protsessi rakendamise eest vastutavale IS juhtkonnale. Kui JSP läbivaatusel avastatud nõrkusi peetakse olulisteks või kaalukateks, tuleks täitevjuhtkonna vastavale tasemele soovitada viivitamatult rakendada parandusmeetmeid.

G32 Jätkusuutlikkuse plaani (JSP) läbivaatus IT seisukohalt (jätkub)

7.2.2 Kuna JSP meetmete toimivus sõltub talitluse jätkusuutlikkuse plaanimise protsessist ja sellega seotud meetmetest, tuleks aruandes näidata ka nende meetmete nõrkused.

7.2.3 IS audiitor peaks võtma aruandesse sobivad soovitused meetmete tugevdamiseks eesmärgiga leevendada nendega seotud riske.

8 JÄRELTOIMINGUD

8.1 Õigeaegsus

8.1.1 Harilikult on kõigi JSP nõrkuste toime laiaulatuslik ja suurt riski tekitav. Seetõttu peaks IS audiitor asjakohastel juhtudel sooritama piisava ja õigeaegse järeltöö, kontrollides, kas juhtkond rakendab viivitamatult meetmeid nõrkuste vastu.

8.2 Toimivus

8.2.1 Läbivaatuse toimivusele mõistliku kinnituse saamiseks peaks IS audiitor viima läbi järelläbivaatuse, millega vaadata üle, kas soovitusi on arvestatud, ja kontrollida rakendatud parandusmeetmete toimivust.

9 JÕUSTUMISKUUPÄEV

9.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. septembril 2005 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

G33 Interneti kasutamise üldised kaalutlused

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S4 "Kutsealane pädevus" määrab: "IS audiitor peaks olema kutsealaselt pädev, tal peaksid olema auditiülesande täitmiseks vajalikud oskused ja teadmised."

1.1.2 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.3 Standard S6 "Audititöö sooritamine" määrab: "Auditiprotsess tuleks dokumenteerida, kirjeldades sooritatud auditööd ja auditi asitõendeid, mis toetavad IS audiitori leide ja järeldusi."

1.2 Seos täiendavate suuniste ja protseduuridega

1.2.1 Suunised

- G22 – Ettevõtte ja kliendi vahelise (B2C) e-äri läbivaatus
- G24 – Interneti-pangandus

1.2.2 Protseduurid

- P2 – Digitaalallkirjad ja võtmehaldus
- P3 – Sissetungi avastamise süsteemide ülevaade
- P6 – Tulemüürid
- P8 – Turvalisuse hindamine. Läbistustestimine ja nõrkuste analüüs
- P9 – Krüpteerimismetoodikate halduse meetmete hindamine

1.3 Seos COBITiga

1.3.1 Konkreetse auditi käsitlusalale rakendatava kõige asjakohasema materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ning COBITi juhtimiseesmärkide ja nendega seotud juhtimistavade arvestamisel.

IS audiitorite kohustuste, õiguste ja vastutuse nõuete täitmiseks

on tõenäoliselt kõige asjakohasematena valitavad ja kohaldatavad COBITi protsessid alljärgnevas loetelus jagatud esmasteks ja teisesteks. Protsessid ja juhtimiseesmärgid, mis tuleb valida, võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest.

1.3.2 Esmajärjekorras

- S2 – Hinnata sisejuhtimise adekvaatsust (COBIT v3)
- S3 – Saada sõltumatu kinnitus (COBIT v3)
- S4 – Korraldada sõltumatu audit (COBIT v3)

G33 Interneti kasutamise üldised kaalutlused (jätkub)

1.3.3 Teises järjekorras

- PO6 – Teavitada juhtimissihid ja suund
- PO7 – Hallata IT inimressursse
- PO8 – Tagada vastavus välisnõuetele (COBIT v3)
- TT1 – Määratleda teenusetasemed ja hallata neid
- TT2 – Hallata kolmandate osapoolte teenuseid
- TT10 – Hallata probleeme
- S1 – Seirata protsessi (COBIT v3)

1.3.4 JSP läbivaatuse jaoks kõige asjakohasemad teabekriteeriumid on

- esmajärjekorras toimivus, tõhusus ja konfidentsiaalsus;
- teises järjekorras käideldavus, terviklus ja usaldatavus.

1.4 Suunise vajadus ja eesmärk

1.4.1 Kiiresti muutuvale infotehnoloogiale, temaga seotud nõrkustele ja potentsiaalsetele turvaaukudele reageerimisel on IS audiitoritel oluline roll. Selle suunise eesmärk on kirjeldada Interneti kasutamise, Internetti pääsu ja/või Interneti-ühenduste läbivaatuse sooritamiseks soovitatavaid tavasid. Asjakohaste juhtimiseesmärkide saavutamiseks organisatsiooni varade kaitsel peaks IS audiitor olema võimeline välja selgitama, dokumenteerima, testima ja hindama turvameetmeid ja nendega seotud riske.

1.4.1 See suunis annab juhiseid IS auditeerimise standardi S6 "Audititöö sooritamine" rakendamise kohta nii, et Interneti-ühenduste läbivaatusel saadaks piisavaid, usaldatavaid, asjassepuutuvaid ja kasulikke asitõendeid. IS audiitor peaks suunist arvestama otsustamisel, kuidas jõuda ülalnimetatud standardi rakendamiseni, kasutama selle rakendamisel kutsealast otsustusvõimet ning olema valmis põhjendama iga lahknevust.

1.4.2 Internet muutub üha enam ettevõtte infrastruktuuri osaks ja teda kasutatakse sageli mitmeks otstarbeks. Üldiselt võib Interneti kasutamise jagada neljaks. Internetti võidakse kasutada

- teabe kogumise ja ühiskasutuse allikana;
- sidekanalina;
- ettevõtteid, organisatsioone või isikuid tutvustava aknana;
- elektroonilise turuna, kus kaubelda.

See suunis hõlmab Interneti kasutamist eeskätt sidekanalina ning ettevõtete ja organisatsioonide teabeallikana. Teatud määral käsitleb suunis Internetti ka tutvustus- ja kauplemiskanalina.

G33 Interneti kasutamise üldised kaalutlused (jätkub)

1.4.3 Internetiga ühendumisel on ettevõte avatud paljudele ohtudele. Nende ohtudega toimetulemiseks on oluline teha riskianalüüsi ja rakendada vajalikke turvavaid ettevaatusabinõusid. Tähtis on ka teadvustada seda, et Internet ei ole staatiline. Ta muutub tihti ning sead teevad ka ohud ja turvameetmete vajadus.

1.4.4 Iga teenuse puhul on toodud näiteid mitmesuguste ohtude kohta. Nii üldine ja lühike dokument ei kata riskipilti täielikult. Ilmub uusi häkkerite tööriistu ja pidevalt tuleb ilmsiks uusi turvanõrkusi IT-süsteemides. Seetõttu on tähtis enne Internetiga ühendumist saada ajakohast teavet ohtude ja turvameetmete kohta.

1.4.5 Interneti kasutamisega pole seotud mingit üldist ega rahvusvahelist tsentraliseeritud juhtimist. Vajalike turvameetmete rakendamine jääb iga üksiku ettevõtte hooleks.

1.5 Suunise rakendamine

1.5.1 Selle suunise rakendamisel peaks IS audiitor arvestama ta juhiseid seoses muude asjassepuutuvate ISACA standardite, suuniste ja protseduuridega. Aja edenedes ei tarvitse see suunis enam olla ammendav ega ajakohane.

2 ÜLDISI KAALUTLUSI INTERNETI-ÜHENDUSTE PUHUL

2.1 Internetiga ühendamise viisid

2.1.1 Internetiga ühendamiseks on mitu moodust ja igal neist on erinev turvameetmete vajadus. Järgnevas on mõned näited.

- Lahus PCd modemitega, mis on ühendatud Interneti-teenuseandja (ISP) kaudu.
- PCd kohtvõrkudes, modemitega, mis on Internetiga ühendatud ISP kaudu.
- Lahus PCd mobiil-andmesideühendustega.
- PCd kohtvõrkudes, mobiil-andmesideühendustega.
- Kohtvõrgud, mis on Internetiga ühendatud marsruuteri kaudu.
- Kohtvõrgud, mis on Internetiga ühendatud tulemüüri kaudu.
- Kaks eraldi võrku: üks on kohtvõrk PCdega, mida kasutatakse organisatsiooni tegevusteks, ja teine võrk PCdega Interneti-suhtluseks.

2.1.2 Mõningaid neist ühendustest võidakse kombineerida teenuse andmisega või Interneti kasutamisega teabekanalina. Näiteid:

- kohtvõrk, mis on ühendatud Internetiga ja pakub kohtvõrgus asuvalt serverilt sisemisi või väliseid teenuseid;
- kohtvõrk, mis on ühendatud Internetiga ja pakub sisemisi või väliseid teenuseid serverilt, mis on paigaldatud demilitariseeritud tsooni;

- kaks sama ettevõtte kohtvõrku, mis on ühendatud Interneti kui sidekanali kaudu;
- organisatsiooni kohtvõrk, mis on ühendatud koostööpartneri võrguga ja sidekanalina kasutatakse Internetti (partnervõrk ehk ekstranet).

2.2 Ohud

2.2.1 Kinnises, ilma välisühendusteta võrgus kuuluvad üldiselt ohtude hulka tehnilised rikked, kasutaja vead, süsteemide väärkasutus või ebalojaalsete töötajate sooritatav konfidentsiaalse teabe levitamine. See riskipilt muutub, kui ettevõte ühendab end püsivalt Internetiga.

2.2.2 Ründed võib jagada järgmistesse gruppidesse.

- Passiivsed ründed, näiteks järgmised.

  - Võrgu seire: Interneti kaudu edastatavate kasutajanimede ja paroolide lugemine nuhkvara abil.

  - Andmepüük: konfidentsiaalse teabe hankimine siseneva või väljuva meili lugemise või kopeerimise teel.

  - Luuretarkvara kasutamine: väga mitmesuguse kahjurvara kasutamine arvuti töö jälgimiseks või selle juhtimise osaliseks ülevõtmiseks ilma kasutaja teadliku nõusolekuta. Harilikult nakatab kasutajaid teatavate veebisaitide külastamine.

- Aktiivsed ründed, näiteks järgmised.

  - Katsed saada juurdepääsu turvameetmete nõrkuste kaudu. Volitamata pöördumine kohtvõrkude ja sisemiste IT-süsteemide poole, kui turvameetmeid ei rakendata õigesti.

  - Paroolide hankimine: priivara kasutamine juurdepääsuks paroolifailidele.

  - Maskeraad: Usaldatava võrguaadressi konfigureerimine arvutile, et saada juurdepääsu konfidentsiaalsele teabele.

  - Viirustega nakatamine: levitatakse kahjurkoodi, mis viib end IT-süsteemi ja sageli levib süsteemi töötamisel teistesse süsteemidesse ja arvutitesse.

  - Trooja hobune: kasutatakse kahjurprogrammi, millel näib olevat mingi kasulik otstarve, kuid mis kannab viirust või operatsiooni, mis püüab paroole, mida saab kasutada volitamata juurdepääsuks süsteemile.

  - Ussidega nakatamine: kasutatakse kahjurkoodi, mis levib ühest IT-süsteemist teise ilma kasutaja toiminguteta.

  - Operatsioonisüsteemi ja rakenduste defektide ja nõrkuste ärakasutamine. Enamikus süsteemides leiduvaid defekte ja nõrkusi kasutatakse volitamata toimingute sooritamiseks.

  - Vääralt konfigureeritud IT-süsteemide ja sideseadmete ärakasutamine: süsteemidele saadakse juurdepääs süsteemiadministraatorite tehtud vigade tõttu süsteemide konfigureerimisel või konfiguratsiooni ajakohastamata jätmise tõttu pärast uue tarkvara või riistvara installeerimist.

G33 Interneti kasutamise üldised kaalutlused (jätkub)

- Teenuseründed, näiteks järgmised.

- Katsed peatada või välistada teenust. Kasutatakse ära andmevoogudes olevad vead ja edastatakse andmekoguseid, mis on selle teenuse jaoks liiga suured. Tulemuseks võib olla andmeummistus.

- Süsteemi suutvuse hõivamine. Süsteemide suutvuse vähendamiseks saadetakse pidevaid päringuid võrguteenusearvutitele, mis ei ole korralikult konfigureeritud.

- IT-süsteemide töö lõpetamine. Andmeummistuse põhjustamiseks koormatakse arvuti üle, saates talle liiga suuri andmekoguseid, mida ta ei suuda käsitleda. Süsteemi töö ootamatuks lõpetamiseks (teenusetõkestuseks, DoS) on palju mooduseid.

- Tehingute ümbermarsruutimine. Kopeeritakse teenuseandja kodulehed kaugserverile, millele on konfigureeritud teenuseandja aadress, et saada e-äri tehingutest krediitkaardinumbrid.

- Suhtlusosavus. Usaldatavat partnerit teeseldes mõjutatakse volitatud kasutajat juurdepääsu saamiseks konfidentsiaalsetele ärisaladustele või teabele kasutajanimede ja paroolide kohta.

2.3 Interneti-teenused

2.3.1 Saadaval on mitmeid Interneti-teenuseid ja uusi teenuseid ilmub tihti. Praegu on kõige populaarsemad teenused

- e-post,
- ülemaailmne veeb (WWW),
- failiedastusprotokoll (FTP),
- uudisegrupid,
- Telnet ja interaktiivne kaugpöördus,
- Internetivestlus (IRC) ja kiirsõnumside.

2.3.2 E-post on kõige sagedamini kasutatav teenus Internetis. See teenus on oma kiiruse, odavuse ja kasutajasõbralikkuse tõttu hakanud üha enam asendama tavalisi kirju ja faksi. E-post ei olnud mõeldud turvalise teenusena ning tal on mitmeid turvanõrkusi. Kõige märgatavamad nõrgad kohad on järgmised.

- Saatja. Keegi ei või olla kindel, et meili päises näidatud saatja on tegelik saatja. Nime on lihtne vahetada ja saatja identiteedi kontroll puudub. Selle nõrkuse saab kõrvaldada digitaalallkirjade abil; neid kasutatakse tihti äripartnerite vahel, kuid meilide vahetamisel juhuslike poolte vahel ei ole see vahend levinud.
- Avatekstiga sõnumid. Interneti kaudu saadetakse sõnumid avatekstina. See võimaldab kõigil Interneti kasutajail sõnumit lugeda ja muuta. Kunagi ei või olla kindel, et sõnum kulgeb muutumatult läbi Interneti. Selle nõrkuse saab kõrvaldada sõnumi krüpteerimisega.

G33 Interneti kasutamise üldised kaalutlused (jätkub)

- Sõnumite kohaletoimetus. Veel üks meili nõrkus on selles, et pole mingeid kindla kohaletoimetuse garantiisid. Harilikult toimetatakse sõnum kohale mõne sekundi või mõne minutiga, kuid mõnikord võib see kesta tunde, kui sõnum üldse kohale jõuabki. Kui üks serveritest edastusahelas ei ole mingil põhjusel käideldav, võivad sõnumid jääda sellele serverile, kuni ta on taas võrgus. Harilikult saab saatja teate nurjumise kohta alles mõne aja pärast, sõltuvalt sellest, kuidas meilisüsteem on konfigureeritud. Enamikul meilisüsteemidest on postitusfunktsiooni sertifikaat. Eri meilisüsteemide ühildamatuse tõttu võib aga tagasiside jääda saamata.
- Manused. Interneti kaudu meili kasutavatest ettevõtetest võimaldab enamik lisada meilile manuseid. Kui need manused on suured, ummistavad nad meilisüsteemi ja serveri, nii et meili kasutajail tõkestatakse muu meili saamine. Sellise olukorra vältimiseks võib ettevõte seada saabuda lubatava meili manuste mahule kitsendused ning anda suuniseid meilide arhiveerimise ja kustutuse kohta.
- Rämpspost. Üha kasvav probleem on soovimatud meilid; neid nimetatakse rämpspostiks ehk spämmiks. Need võivad olla soovimatud reklaamid ja teenusepakkumused, sealhulgas sellised toodete pakkumised, mis võivad olla häirivad. Selline rämpspost täidab serverid ja röövib saajate aega. Rämpsposti ei loeta otseselt turvaprobleemiks, kuid ta võib vähendada IT-süsteemide käideldavust.

2.3.3 WWW on ülemaailmne serverite võrk, mis pakub teavet lihtteksti, heli ja piltidena. Rahvusvahelisele kasutajaskonnale on kättesaadavad mitmesugused teenused, näiteks rahandusteenused ja kaubandus. WWW poole pöördutakse brauseri (näiteks Internet Explorer, Opera jt) kaudu.

- Teabe kvaliteet. WWW sisaldab tohutul hulgal teavet, kuid selle teabe kvaliteet varieerub. WWWsse paigutatava teabe üle pole mingit kõrgemat kontrolli. Kvaliteedi tagamise eest vastutab igaüks, kes paigutab teavet WWWsse. Seetõttu pole mingit teabe usutavuse, täpsuse ega värskuse garantiid.
- Jäljed. Veebisaitide külastamisel jätab Interneti kasutaja endast mitmeid jälgi, eelkõige võrguaadressi, kuid mõnikord ka kasutajanime. Kui ta külastab organisatsiooni arvuti kaudu sobimatuid saite Internetis ja jätab endast jälgi, võidakse organisatsiooni seostada selliste veebisaitidega, mis näiteks pakuvad pornograafiat, äärmuslikke poliitilisi liikumisi jms. Seetõttu eelistavad paljud ettevõtted blokeerida niisuguste veebisaitide aadressid.
- Brauser. Saadaval on palju brausereid, mitmesuguste funktsioonide, tugevuste ja nõrkustega. Sageli avastatakse brauserites uusi turvanõrkusi. Mõned neist nõrkustest võivad ettevõtetele tekitada tõsiseid probleeme. Arvutikelmid võivad luua kodulehti, mis sisaldavad kahjurkoodi, mis kasutab ära turvanõrkused ja käitab organisatsiooni PCdel volitamata töid.
- Lisandmoodulid. Enamkasutatavates brauserites on võimalik installeerida väikesi lisaprogramme (plugin), mis lisavad suuremaid võimeid, näiteks täiuslikumat heli, laiendatud videofunktsioone või mänge. Programmeerimisvead mõnedes lisamoodulites on võimaldanud sissetungijail saada juurdepääsu IT-süsteemides olevatele andmetele.

G33 Interneti kasutamise üldised kaalutlused (jätkub)

- Prääniku (*cookie*). Väikesed teabejupid, mida kasutab brauser ja mis edastatakse kõvakettale logimise ja dokumenteerimise otstarbeks; näiteks viimase WWW külastuse kuupäev, külastatud kodulehed ja ostetud tooted (kui külastati mingit e-kauplust). E-kauplused põhinevad sageli prääniku kasutamisel. Prääniku võivad ka salvestada paroole; prääniku kasutamine ei kujuta endast siiski mingeid teadaolevaid turvaohte, pigem võib neid pidada privaatsuse rikkumiseks, sest veebisaidid salvestavad teavet kasutajate ja kasutajatoimingute kohta. Kas lubada kasutada prääniku või mitte, on poliitikaküsimus. Enamikus brauserites on võimalik valida, kas lubada prääniku või mitte. Saadaval on ka priivara, mis annab võimaluse kasutada prääniku Internetis surfimise ajal, kuid kõrvaldab väljalogimisel kasutajateabe.

2.3.4 FTP on teenus, mis võimaldab andmete edastust ühest arvutist teise. Sageli kasutatakse seda failide allalaadimiseks WWWst. FTP on põhiliselt ebaturvaline. Kasutajanimed ja paroolid edastatakse läbi võrgu avatekstina. FTP kasutamisel on väga tähtis konfigureerida see teenus õigesti. FTP-teenuse erijoonte hulka kuuluvad järgmised.

- Anonüümne FTP. Teenus, mis võimaldab väljaspoolsetel ettevõtte serverilt alla laadida andmeid või programme. Kui ettevõtte soovib seda teenust pakkuda, on väga tähtis konfigureerida süsteemid õigesti. Kui ta seda ei tee, võivad sissetungijad saada juurdepääsu ettevõtte andmetele. Samuti saab seda serverit kasutada ka ebaseaduslike andmete või programmide talletuseks. Sellistel juhtudel logib kasutaja end sisse kasutajanimega (anonymous või ftp). Vähe on aga neid süsteeme, mis kontrollivad, kas kasutajanimi (harilikult on selleks meiliaadress) ja parool on õiged.
- Aktiivne ja passiivne side. Erinevalt teistest teenustest kasutab FTP sideks kaht lüüsi. Peale selle saab ühenduse luua kahel viisil, aktiivse või passiivsena. Aktiivse side puhul otsustab kasutaja, millist lüüsi kasutada. Selles režiimis on võimalik andmete vastuvõttu juhtida ja filtreerida. Passiivse režiimi puhul otsustab ühendatud server, millist lüüsi kasutada. Passiivset režiimi on paljudel tulemüüridel raske turvaliselt käsitleda.

2.3.5 Uudisegrupp on omamoodi teatetahvel, kus kasutajad saavad arutada suvalisi küsimusi. Kui uudisegruppi saadetakse kiri, paigutatakse see teatetahvlile koos saatja nime ja aadressiga. Sageli levitatakse kirja eri uudiseserveritele üle kogu maailma. Seetõttu on uudisegruppi saabunud kirja peaaegu võimatu kõrvaldada. Kui kiri saadeti organisatsiooni arvutilt, võidakse seda pidada organisatsiooni ametlikuks seisukohaks. On ka risk, et töötaja võib avaldada organisatsiooni saladusi. Juurdepääsu uudisegruppidele on võimalik blokeerida. See on organisatsiooni poliitika küsimus.

2.3.6 Telnet on teenus, mis võimaldab sisse logida teistesse võrgu arvutitesse. Telnet annab kasutajale märgipõhise virtuaalterminali. Sisselogimisel saadetakse kasutajanimi ja parool avatekstina. Sissetungijail on üsna lihtne lugeda kasutajateavet ja kasutada seda lubamatuks juurdepääsuks. Selle vältimiseks võib kasutada ühekordseid paroole ja krüpteerimist. Häkkerid saavad ka hõivata terminaliühenduse (kaaperdada seansi). Pärast kasutaja sisselogimist võtab häkker kasutajapöörduste

seansi üle. Seda saab vältida krüpteerimisega. Oodatavasti lähevad Telneti ülesanded üle sellistele tegelikele kaugpöördusmeetoditele nagu interaktiivne kaugpöördus SSH-ga, kaug-X-windows VNC ja Remote Desktop.

2.3.7 IRC ja kiirsõnumside on reaalaja-konverentsisüsteemid. Kasutajad suhtlevad ühise ala (kanali) kaudu, kus kõik kasutajad saavad osaleda aruteludes. Paljudel IRC ja kiirsõnumivahetuse programmidel on turvanõrkusi, mis võimaldavad sissetungijail saada ebaseadusliku juurdepääsu organisatsiooni failidele. Sissetungijad võivad neid kanaleid kasutada ka viiruste levitamiseks ning juurdepääsu saamiseks suhtlusosavusega.

3 TURVAMEETMED

3.1 Poliitika, tooted ja järeltoimingud

3.1.1 Turvalised Interneti-ühendused tuleks rajada ettevõtte infoturbepoliitikale. On tähtis, et kehtiksid suunised Interneti õige ja turvalise kasutamise tagamiseks ja et turvateadlikkus oleks üks tähtsamsid juhtimissihte. Kui töötajad ei järgi neid suuniseid, ei hakka turvameetmed toimima ootuspäraselt. Kasutusel peaksid olema volitamise ja muudatusehalduse protseduurid. Peale selle peaksid turvasuunised hõlmama eetilist käitumist Interneti kasutamisel.

3.1.2 Turul on palju tooteid, millega saab tõsta Interneti turvalisust. Õige turvataseme saavutamiseks on vaja rakendada mitut toodet, mis täiendavad üksteist. Toodete valimine peaks põhinema riski kaalutlemisel.

3.1.3 Väga tähtis on turvameetmete jälgimine. Kasutusel peaksid olema turvameetmete seire ja järeltoimingute tööjuhendid, millega tagada meetmete toimivus ja vastavus suunistele.

3.2 Tulemüürid

3.2.1 Tulemüür on levinuim turbevahend, mida kasutatakse ühenduse loomisel kohtvõrgust Internetti. Tulemüür on riistvara ja tarkvara kombinatsioon, mis väldib ebaseaduslikke sissetunge. Tulemüür peaks kajastama ettevõtte turvapoliitikat. Läbi tulemüüri peaksid kulgema ainult lubatavad teenused.

3.2.2 Tulemüüriks võib olla üks järgmistest.

- Pakette filtreerivad marsruuterid. Uurivad võrku sisenevaid või sealt väljuvaid andmepakette.
- Rakenduslüüsid. Kohaldavad turvamehhanisme konkreetsetele rakendustele, näiteks FTP-le või Telnetile.
- Kanalitaseme lüüsid. Rakendavad turvamehhanisme TCP- või UDP-ühenduse loomisel.
- Vaheserverid (proksid). Hõivavad sõnumeid, mis sisenevad võrku või väljuvad sealt, ning võimaldavad peita tegeliku IP-aadressi.

G33 Interneti kasutamise üldised kaalutlused (jätkub)

Kasutatav tulemüür võib olla tarkvarapõhine või riistvarapõhine; viimane on mõeldud eeskätt ärikeskkondadele ning võib rakendada mitut ülalnimetatud meetodit.

3.2.3 Need tulemüürid erinevad pakutava turvalisuse tüübi poolest ning nad vajavad jälgimist ja hooldust.

3.2.4 Tulemüüri läbivate andmete reguleerimiseks on kaks turvakontseptsiooni:

- kõike kitsendatakse täielikult: läbi pääsevad ainult teenused, mida lubab juhtkond;
- üldisi kitsendusi ei ole: läbi ei lasta ainult neid teenuseid, mille riske juhtkond loeb suureks.

3.2.5 Tulemüüri lahenduse valimisel tuleks arvestada ettevõtte turbevajadusi, kasutajasõbralikkuse nõuet ja IT-üksuse võimsust. Enne kui kasutajad saavad pääsu Internetti, tuleks tulemüür konfigureerida õigesti ja vastavalt turvapoliitikale.

3.3 Ühekordne parool

3.3.1 Saadaval on palju programme, millega saab paljastada paroole. Selliseid programme kasutavad arvutikelmid ja häkkerid. Sageli võtavad kasutajad paroole, mida on lihtne ära arvata ja kasutada lubamatutel eesmärkidel. Paljastada saab aga ka häid, raskesti äraarvatavaid paroole. Praegused arvutid on nii võimsad, et on võimalik paljastada ka kõige keerulisemaid paroole. Sissetungijate juurdepääsu vältimiseks ettevõtte süsteemile on üks võimalikke lahendusi ühekordsete paroolide kasutamine. Neid saab genereerida parooligeneraatorida või pretensiooni ja vastuse süsteemiga, mis põhineb numbritel, mida saadakse kalkulaatoritaolisest seadmest. Turvalise lahenduse saamiseks on soovitatav kombineerida ühekordseid paroole krüpteerimistarkvaraga.

3.4 Läbistustestimine ja testimistarkvara

3.4.1 Soovitatav on uurida veebirakenduste praegu teadaolevaid nõrkusi, sest nende nõrkuste keerukus ja tõsidus üha kasvab. On rohkesti tarkvara, nii äriliste toodetena kui ka priivarana, mida saab kasutada IT-süsteemide testimiseks eesmärgiga leida mitmesugust tüüpi nõrkusi ja turvaauke. Mõningase osa sellest tarkvarast on välja töötanud väärikad inimesed või firmad, kes tahavad anda oma panuse turvalisema Interneti heaks. Enamiku neist programmidest on aga välja töötanud arvutikelmid sissemurdmiseks ettevõtete süsteemidesse. Usaldatavat läbistustestimise tarkvara kasutades on võimalik testida ettevõtte Interneti-ühenduse turvameetmete kvaliteeti.

3.5 Sissetungi tuvastuse ja vältimise süsteemid

3.5.1 Sissetungi tuvastuse süsteeme (IDS) kasutatakse kohalike võrkude ja töösüsteemide analüüsimiseks eesmärgiga avastada ebaseaduslikud ründed enne kahjustuse tekkimist. IDS avastab kõik tuntud ründed nende toimumise ajal ja saadab teateid ettevõtte IT-personalile või turvajuhile, kes saab rakendada turvameetmeid. Pärast uute ohtude või rünnete avastamist tuleks IDS kiiresti ajakohastada.

3.5.2 Sissetungi vältimise süsteemid (IPS) erinevad teistest turvavahenditest, mis ründe tuvastamiseks selle toimumise ajal (või pärast seda) toetuvad ründe käekirja failidele; sissetungi vältimise tarkvara ennustab rünnet enne selle toimumist. Selleks jälgib ta arvutisüsteemi olulisi kohti ja otsib "halba käitumist", näiteks usside, trooja hobuste, nuhkvara, kahjurvara ja häkkerite oma. Ta täiendab tulemüüre ning viirusetõrje ja nuhkvaratõrje vahendeid, andes täielikumat kaitset tekkivate ohtude eest. Ta suudab blokeerida uusi (sama päeva) ohte, mis mööduvad traditsioonilistest turvameetmetest, sest ta ei sõltu ohtude käekirjade tuvastamisest ja levitamisest ega paikadest.

3.6 Krüpteerimine

3.6.1 Interneti kaudu edastatavad andmed on põhimõtteliselt avatud kõigile. See tähendab, et kaitsmata tundlikke andmeid saab kinni püüda ja ebaseaduslikult kasutada. Üks meetod süsteemi tervikluse ja konfidentsiaalsuse tagamiseks on krüpteerimine. Krüpteerimist saab kasutada eri tasemetel. Kõige turvalisem lahendus on krüpteerimine rakenduse tasemel; see tähendab, et konfidentsiaalsus ja terviklus säilitatakse kogu teel kuni lõppkasutajani. See lahendus aga sõltub kasutajate vahelise tarkvara vastavusest.

3.7 Digitaalallkirjad

3.7.1 Digitaalallkirjade abil saab säilitada sõnumi tervikluse. Eriti kasulik on see Interneti kaudu kauplemisel. Digitaalallkirjad põhinevad võtmepaaridel, mis koosnevad privaatvõtmest ja avalikust võtmest.

3.7.2 [---] [1]

3.8 Virtuaalne privaatvõrk (VPN)

3.8.1 VPN on vahend turvalise sidekanali loomiseks kahe või enama arvuti vahel läbi ühe või mitme ühiskasutatava ebaturvalise füüsilise võrgu. Arvutid võivad olla võrkudega füüsiliselt ühendatud, kuid omavahel saavad andmeid vahetada ainult ühe ja sama virtuaalvõrgu liikmed. Sidekanaleid saab turvata krüpteerimisega.

3.9 Viirusetõrje programmid

3.9.1 Arvutiviirused on üha suurem probleem, eriti pärast makroviiruste ilmumist. Viirused levivad mitmesuguste allikate kaudu, sealhulgas e-kirjade, mängude piraatkoopiate ja Internetist allalaaditud programmide kaudu. Kõigil ettevõtteil, kes

[1] Järgnev tekstilõik on jäetud tõlkimata, sest
1) siin püütakse kirjeldada mitte tüüpilist ja standardset digitaalsignatuuri protsessi (millel põhineb näiteks Eesti ID-kaart), vaid signeerivat krüpteerimist (signcryption);
2) kirjeldus ei saavuta pealegi oma eesmärki kirjeldaja halva inglise keele ja nähtavasti ka krüptograafia-alaste teadmiste puudulikkuse tõttu.
ISACA peaks pöörduma ala asjatundja poole ja selle osa tekstist asendama.
(Tõlkija m.)

saavad manustega meili või lubavad oma töötajail Internetist alla laadida, peaks serveritel ja /või PCdel olema viirusetõrje tarkvara. Väga tähtis on hoida käigus protseduure viirusetõrje tarkvara hoidmiseks ajakohasena.

3.10 Nuhkvaratõrje programmid

3.10.1 Nuhkvara erineb viirustest ja ussidest selle poolest, et tavaliselt ta ei paljune ise. Nagu paljud uuemad viirusedki, on nuhkvara mõeldud nakatatud arvuteid ära kasutama ärilise kasu saamiseks. Tüüpilisi taktikaid selle sihi saavutamiseks on soovimatute hüpikreklaamide saatmine, isikuteabe (sealhulgas rahandusliku, näiteks krediitkaardinumbrite) vargus, veebisirvimise seire turunduslikel eesmärkidel ja HTTP-päringute ümbermarsruutimine reklaamisaitidesse. Sellistele ohtudele avatuse vältimiseks peaks iga ettevõte installeerima nuhkvaratõrje programmid, mis on määratud blokeerima või kõrvaldama nuhkvara.

3.11 Logimine ja seire

3.11.1 Interneti-liikluse logimine ja seire ei ole iseenesest turvameetmed, kuid nad on eeltingimused rünnete avastamiseks ning turvalisuse säilitamiseks võrkudes ja töösüsteemides. Logimise ja seire toimivuse saavutamiseks tuleks neid sooritada sidesõlmedes, näiteks tulemüüris. Järelmeetmeid nõudvad sündmused tuleks määrata riski kaalutlemise ja ettevõtte poliitika põhjal. Logimise tulemusena tekivad suured andmehulgad, mida on raske käsitsi töödelda. Seetõttu on praktiline hankida mingi instrument või tarkvara, millega filtreerida, analüüsida ja esitada asjassepuutuvad logiandmed.

4 INTERNETI KASUTAMINE ETTEVÕTTE TUTVUSTAMISE KANALINA

4.1 Interneti kasutamine vaateaknana

4.1.1 Internetti on kasutatud ettevõtte vaateaknana juba alates WWW ilmumisest. See suunis ei käsitle seda, kuidas tutvustada ettevõtet, vaid esitab mõningaid kaalutlusi selle kohta, mida tuleks arvestada enne teabe edastust WWW-sse ja pärast seda.

4.2 Enne teabe edastust WWW-sse

4.2.1 Enamikule ettevõtteist näib olevat möödapääsmatu olla esindatud WWW-s. Sageli paigutatakse teave kodulehtedele, ilma et pööratakse tähelepanu turvaaspektidele. Kui ettevõte annab detailset teavet oma tegevuse ja töötajate kohta, on ta avatud arvutikelmide suhtlusosavusele. On ka näiteid sellest, et arvutikelmid murravad sisse veebiserveritesse ja muudavad kodulehe sisu.

4.2.2 Enne kodulehe väljatöötamist peaks ettevõte tegema vajaduste analüüsi, mille taustal saaks otsustada, missugust teavet on sobiv esitada, ning määrama ettevõttele nende andmete esitusest tuleneva riski taseme.

G33 Interneti kasutamise üldised kaalutlused (jätkub)

4.3 Pärast teabe edastust WWW-sse

4.3.1 Üldine huvi värskendamata jäänud kodulehtede vastu kaob peagi. Hooldamine ja arendus on väga olulised. Peale selle tuleks serverit iga päev jälgida võimalike ebaseaduslike või volitamata toimingute avastamiseks. Kui arvutikelmid saavad juurdepääsu, saavad nad kodulehe sisu mitmeti muuta. Näiteks võib telefoninumbri asendamine konkurendi numbriga põhjustada kodulehe omaniku müügitulu vähenemist. Kui on olemas juurdepääs WWW-le, on ka võimalik vahetada tarkvara piraatkoopiaid või kasutada serverit ebaseadusliku teabe hoidmiseks.

4.4 Internet kui kauplemiskanal

4.4.1 Kauplemine toodetega Interneti kaudu (e-äri) on teenus, mis kasvab kogu maailmas. See kauplemistegevus sisaldab makseid ja vajab rangeid turvameetmeid. Tarbija peab saama anda müüjale oma krediitkaardi numbri, olles kindel selles, et seda numbrit ei kuritarvitata. Teisalt peab müüja tarbetute kulude vältimiseks või kuritarvituse eest majandusliku vastutuse vältimiseks olema kindel selles, et tellimused on ehtsad.

4.4.2 Turvaliseks kauplemiseks Interneti kaudu on mitu lahendust. Kõige levinumate lahenduste hulka kuuluvad protokollid SSL ("turvaline soklikiht") ja SET ("turvaline elektrooniline tehing").

4.5 Elektrooniline raha

4.5.1 Kauplemine Interneti kaudu on suurendanud turvalise elektroonilise arvelduse vajadust. Paljud ei taha avaldada oma krediitkaardi numbrit ja väikeste summade ülekandmisel ei ole kasulik kasutada krediitkaarte. Seetõttu on mitmed e-kaubanduse firmad töötanud välja lahendusi elektroonilise raha käsitluseks. E-kaubanduse kauplemisahel koosneb kolmest osapoolest; need on klient, müüja ja pank. Enne kui klient saab kasutada e-raha, peab ta pangast alla laadima elektroonilise rahatasku. Selle rahatasku saab installeerida PC-le, pihuarvutile (PDA) või kiipkaardile. Pärast allalaadimist on see raha kasutusvalmis. Tehingute turbeks kasutatakse digitaalallkirju.

4.6 Usaldatav kolmas pool (TTP)

4.6.1 Interneti-põhine kaubandus või ettevõtete elutähtsate andmete või teabe vahetus nõuab tavaliselt jälitatavust. Jälje tervikluse tagamiseks kasutatakse tehingu autentsuse tunnistajatena kolmandaid pooli. Harilikult on nendeks IT alal suured teenuseandjad, kes kasutavad tehnoloogiat, mida nimetatakse avaliku võtme infrastruktuuriks (PKI). Selle peamised funktsioonid on autentimine, krüpteerimine ja digitaalallkiri.

G33 Interneti kasutamise üldised kaalutlused (jätkub)

4.6.2 Mõne viimase aasta jooksul on ilmunud lahendusi, mis võimaldavad ettevõttel endal tulla toime oma turbega, kaasamata kolmandat poolt.

5 AUDITITÖÖ VÕI TURVALÄBIVAATUSE SOORITAMINE

5.1 Plaanimine

5.1.1 IS audiitor peaks õppima tundma organisatsiooni Internetti-pääsu ja Interneti kasutamist. IS audiitor peaks läbi viima Internetti-pääsu ja Interneti kasutamise riskianalüüsi organisatsiooni ja ta missiooni seisukohalt.

5.1.2 Tuleks koostada auditi kava, mis hõlmaks auditi käsitlusala, eesmärke ja ajastust. Aruandluse korraldus tuleks auditi kavas selgelt dokumenteerida. Tuleks arvestada organisatsiooni ja ta huvigruppide iseloomu ja suurust. IS audiitor peaks endale selgeks tegema organisatsiooni missiooni ja tegevuseesmärgid, tehnilise infrastruktuuri tüübid ja tegevuse jaoks elutähtsad andmed.

5.1.3 Vaja on tunda ka organisatsiooni struktuuri, eriti aga keskse personali, sealhulgas teabe haldajate ja omanike rolle ja kohustusi.

5.1.4 Auditi plaanimise järgu esmane eesmärk on tunda ohte ja riske, mis ähvardavad organisatsiooni, kui ühendada ta Internetiga.

5.2 Sooritatavad sammud

5.2.1 IS audiitor peaks kaaluma, kas ühendamine Internetiga põhineb kogu ettevõtte vajaduste hindamisel. Õigete otsuste tegemiseks Interneti kasutamise kohta peaksid nõukogu ja juhtkond olema teadlikud riskidest ja sellest, mida tähendavad ohtude muutused ettevõttele. Läbivaatuse käsitlusala määratlemisel peaks IS audiitor võtma arvesse ka sellised tegurid nagu organisatsioonis mitmesugustel eesmärkidel kogutava, talletatava ja kasutatava teabe tüübid.

5.2.2 IS audiitor peaks välja selgitama, kas organisatsioonis on kasutusel alljärgnev:

- Interneti-poliitika;
- juhis võrguühenduse, tulemüüride jms seire ja järeltoimingute kohta;
- intsidentidest teatamise protseduur;
- kodulehe värskendamise juhis;
- koolitus- ja teadvustuskavad.

Kui need on olemas, peaks IS audiitor neid hindama mõistliku kinnituse saamiseks sellele, et Interneti kasutamine on kooskõlas poliitikate ja protseduuridega.

G33 Interneti kasutamise üldised kaalutlused (jätkub)

5.3 Detailse läbivaatuse sooritamine

5.3.1 IS audiitor peaks hindama järgmisi halduslikke aspekte:

- juhtkonna kohustused;
- Internetti-pääsu andmise eesmärk;
- kas ettevõttel on konfidentsiaalseid või privaatsusandmeid, mille tõttu tuleks pääsu Internetti kitsendada või mitte lubada;
- ühenduse tüüp;
- kas töötajate juurdepääsu aluseks on olnud vajaduste hindamised;
- kas pääs on kitsendatud teatud kellaegade või nädalapäevadega;
- kas on mingeid kitsendusi sellele, kus töötajail lubatakse surfida või teavet koguda;
- kas ettevõte müüb Interneti kaudu tooteid või teenuseid ja kas maksed tehakse Interneti kaudu;
- kas ettevõttel on Interneti-ühenduse installeerimiseks, jälgimiseks ja hoolduseks vajalikku pädevust, aega ja suutvust.

5.3.2 Riski kaalutlemisega tuleks hõlmata vähemalt järgnev:

- ohud;
- ohtude muutused Internetiga ühendumisel;
- kas olemasolev infoturbepoliitika katab Interneti kasutamise;
- kas ettevõte pakub huvi arvutikelmidele või tootmisspionaažile;
- sissetungijaile sisemise või konfidentsiaalse teabe avanemise tagajärjed;
- turvaintsidendi toimumise maksumus;
- turvaintsidendi toimumise tõenäosus;
- turvameetmed, mida tuleb rakendada Interneti-ühenduste kaitseks.

5.3.3 Juhistes Interneti kasutamise kohta peaks olema vähemalt järgnev:

- seos turvapoliitikaga;
- lubatavate teenuste dokumenteering;
- nende teenuste lubatava kasutamise reeglid ja sanktsioonid reeglite rikkumisel;
- õigusnormidele vastavuse võrguseire protseduuride kirjeldus;
- eetiliste hoiakute dokumenteering;
- meili saatmise ja talletuse reeglid;
- kasutajate koolituse nõuded;

G33 Interneti kasutamise üldised kaalutlused (jätkub)

- võimalikud lepped koostööpartneritega;
- Interneti-liikluse logimist ja seiret puudutavate õigusnormise võimalike rikkumiste vältimiseks oluline lepe, millele kirjutavad alla kõik töötajad, kinnitades, et nad on juhiseid lugenud, neist aru saanud ja järgivad neid.

5.3.4 Internetiga töötamise dokumentatsioonis peaks olema käsitletud vähemalt järgnev:

- kogu tehniline seadmestik ja infrastruktuur;
- logimise ja seire eeskirjad;
- alarmide häälestus;
- logimise ja intsidendikäsitluse protseduurid.

5.3.5 Interneti-ühenduse dokumentatsioonis peaks olema vähemalt järgnev:

- võrgu perimeetrite kirjeldus;
- pääsupunktide kirjeldus;
- kõigi modemiühenduste kirjeldus;
- marsruuterite ja võimalike vaheserverite konfiguratsioon;
- tulemüüride konfiguratsioon;
- muude turvameetmete, näiteks krüpteerimise ja digitaalallkirjade konfiguratsioon;
- logifailide turvalise talletuse (näiteks WORM-ketastel, välistel ketastel või lintidel) kirjeldus;
- logifailide taastamise protseduuride kirjeldus.

5.3.6 Seireprotseduuride dokumentatsioonis peaks olema käsitletud vähemalt järgnev:

- Interneti-ühenduse, sealhulgas varundusressursside halduse ja hoolduse kohustuse kirjeldus;
- tulemüüri logifailide läbivaatus;
- käigusolevate serverite tehingute läbivaatus;
- kasutajatoimingute logifailide läbivaatus;
- võrgustatistika läbivaatus;
- võimalike turvaintsidentide või turvalisuse rikkumise katsete käsitlus.

5.4 Kohustused

5.4.1 Kasutajate kohus on

- järgida IS poliitikat, juhiseid ja eetikanorme;
- järgida nende maade õigusnorme, kus teavet kogutakse;

G33 Interneti kasutamise üldised kaalutlused (jätkub)

- mitte teatada parooli telefoni teel või meiliga;
- mitte vahetada paroole tundmatult isikult telefoni teel või meiliga saadud nõudel;
- mitte kasutada Internetis sama kasutajanime ja parooli, mis on kasutusel kohalikus võrgus;
- kontrollida Internetist allalaaditud andmeid enne nende kasutamist tööalaste otsuste, kauplemise, maksete vms alusena.

5.4.2 IT juhtkonna kohustuste hulka kuuluvad järgnevad.

- Interneti tulemüüride, marsruuterite, serverite ja muu kasutuseloleva IT-seadmestiku hooldus ja jälgimine. See sisaldab kohustust tagada süsteemitarkvara ja rakenduste õigete versioonide õiget installeerimist ja hooldust. Peale selle peaks IT juhtkond kindlustama tulemüüri logide igapäevase käsitluse ja konfiguratsiooni vastavuse kirjalikele juhistele.
- Kasutuselolevate süsteemide ja rakendustega seotud uusimate ohtude ja nõrkuste teadmine; see on vajaliku turbetaseme korraliku säilitamise eeltingimus.

5.4.3 Turbe juhtkonna kohustuste hulka kuuluvad järgnevad.

- Infoturbe eest vastutava isiku muude funktsioonide (näiteks IT operaatori, süsteemianalüütiku või programmeerija omade) välistamine.
- Interneti kasutamise juhiste väljatöötamine ning kasutajaile teabe andmine lubatava ja eetilise kasutamise kohta; see on turvajuhi peamine ülesanne.
- Toimimine infoturbe alase ressursina tippjuhtkonna jaoks.
- Tulemüüri logide läbivaatus.
- Turvasüsteemide teadete läbivaatus.
- Turvameetmete regulaarse testimise kindlustamine.
- Hoolitsemine selle eest, et jätkusuutlikkuse ja avariikäsitluse plaanid katavad ettevõtte teenuseid.
- Turvaintsidentide ja turvalisuse rikkumise katsete käsitlus.
- Tõsistest turvaintsidentidest teatamine juhtkonnale.
- Kasutuselolevate süsteemide ja rakendustega seotud uusimate ohtude ja nõrkuste teadmine võrdselt IT juhiga.

5.4.4 Tippjuhtkonna kohustuste hulka kuuluvad järgnevad.

- Üldise Interneti-poliitika sõnastamine.
- Selle poliitika ja temaga seotud protsesside seire.
- Adekvaatsete ressursside eraldamine.
- IT juhtkonnale volituste andmine poliitika elluviimiseks.

G33 Interneti kasutamise üldised kaalutlused (jätkub)

5.5 Tehnilised abinõud ja turvameetmed

5.5.1 Tehniliste abinõude hulka kuuluvad järgnevad.

- Süsteemitarkvaras peaksid turvaalarmid ja lubamatute intsidentide logimine olema aktiveeritud
- Kohtvõrgu ja Interneti vaheline ühendus peaks olema kaitstud tulemüüriga.
- Läbi tulemüüri peaksid kulgema ainult teenused, mida lubab juhtkond.
- Tulemüür peaks peatama kõik lubamatud võrguprotokollid.
- Süsteemi tõrke või tootmise katkemise korral peaks tulemüür peatama igasuguse juurdepääsu.

5.5.2 Teenustega seotud meetmete hulka kuuluvad järgnevad.

- E-post

  - Elutähtsad sõnumid tuleks krüpteerida.

  - Aegkriitilisi sõnumeid tuleks jälgida käsitsi.

  - Manuseid tuleks kahjurkoodist põhjustatud kahjustuste vältimiseks kontrollida.

  - Paroole ei tohiks saata meiliga.

- WWW

  - Interneti-teenuste kasutamisel tuleks kasutada kohtvõrgu omadest erinevaid kasutajanimesid ja paroole.

  - WWW-st allalaaditud teavet tuleks enne kasutamist kontrollida.

  - Kasutada tuleks ainult kinnituse saanud Interneti-brauserit ning ei tohiks lubada muuta selle konfiguratsiooni ega installeerida lisandmooduleid.

  - Kõiki Internetist allalaaditud faile tuleks kontrollida viiruste, nuhkvara jms kahjurkoodi avastamiseks.

- FTP

  - Kõiki Internetist allalaaditud faile tuleks kontrollida viiruste, nuhkvara jms kahjurkoodi avastamiseks.

- Uudisegrupid

  - Kasutajail ei tohiks lasta osaleda fleimisõdades.

  - Kasutajail ei tohiks lubada kirjutada artikleid, mis võivad tekitada negatiivse mulje ettevõttest, selle töötajaist, koostööpartnereist, tarnijaist või konkurentidest.

  - Uudisegruppidest kogutud teavet tuleks enne kasutamist kontrollida.

- Telnet

  - Kui võimalik, tuleks kasutada ühekordseid paroole.

G33 Interneti kasutamise üldised kaalutlused (jätkub)

- IRC ja kiirsõnumivahetus

  - IRC ja kiirsõnumivahetus peaksid olema lubatud ainult autonoomselt PC-lt.

  - IRC ja kiirsõnumivahetuse kasutamisel ei tohiks olla lubatav anda ettevõtte sisemist teavet.

5.5.3 Muude turvameetmete hulka kuuluvad järgnevad.

- Sisselogimiseks kodusest töökohast või muust välisest asukohast tuleks kasutada VPN-ühendust turvalise autentimisega, näiteks ühekordse parooliga.
- Väliskasutajatele spetsialiseeritud serverid tuleks installeerida demilitariseeritud tsoonis (DMZ).
- CGI skriptid ja muu kasutatav kood, mis võtab vastu andmeid Internetist, peaks olema kvaliteedikinnitusega ning testitud vigade ja nõrkuste avastamiseks.

6 JÕUSTUMISKUUPÄEV

6.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. märtsil 2006 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

G34 Kohustused, õigused ja vastutus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S1 "Audititalituse põhikiri" määrab: "Infosüsteemide auditi talituse või infosüsteemide auditi ülesande täitja eesmärk, kohustused, õigused ja vastutus peaksid olema auditi põhikirjas või töövõtukirjas asjakohaselt dokumenteeritud."

1.1.2 Standard S3 "Kutse-eetika ja standardid" määrab: "IS audiitor peaks järgima ISACA kutse-eetika koodeksit."

1.2 Seos COBITiga

1.2.1 Lai juhtimiseesmärk S3 ("Saada sõltumatu kinnitus", COBIT v3) määrab: "... saada sõltumatu kinnitus organisatsioonide, klientide ja kolmandatest pooltest tarnijate vahelise usalduse ja usaldusväärsuse suurendamiseks."

1.2.2 Lai juhtimiseesmärk S4 ("Korraldada sõltumatu audit", COBIT v3) määrab: "... korraldada sõltumatu audit usalduse suurendamiseks ja parimate tavade alastest nõuannetest kasu saamiseks."

1.2.3 Detailne juhtimiseesmärk S4.1 ("Audititalituse põhikiri", COBIT v3) määrab: "Organisatsiooni kõrgem juhtkond peaks kehtestama audititalituse põhikirja. See dokument peaks visandama audititalituse kohustused, õigused ja vastutuse. Põhikirja tuleks perioodiliselt läbi vaadata, nii et see tagaks audititalituse sõltumatuse, õigused ja kohustused.

1.3 Toetumine COBITile

1.3.1 Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ning arvestades COBITi teabekriteeriume ja nendega seotud juhtimistavasid. Selle nõude täitmiseks on COBITist valitud ja sobitatud tõenäoliselt kõige asjakohasemad protsessid ning need on alljärgnevas liigitatud esma- ja teisejärgulisteks. Valitavad ja sobitatavad protsessid ja juhtimiseesmärgid võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest.

1.3.2 Esmajärgulised

- SH2 – Seirata ja hinnata sisejuhtimist
- S3 – Saada sõltumatu kinnitus (COBIT v3)
- S4 – Korraldada sõltumatu audit (COBIT v3)

1.3.3 Teisejärgulised

- PO6 – Teavitada juhtimissihid ja suund
- PO7 – Hallata IT inimressursse
- P08 – Tagada vastavus välisnõuetele (COBIT v3)

G34 Kohustused, õigused ja vastutus (jätkub)

- TT1 – Määratleda teenusetasemed ja hallata neid
- TT2 – Hallata kolmandate osapoolte teenuseid
- TT10 – Hallata probleeme
- S1 – Seirata protsessi (COBIT v3)

1.3.4 Kohustuste, õiguste ja vastutuse puhul kõige asjassepuutuvamad on järgnevad teabekriteeriumid:

- esmajärjekorras toimivus, tõhusus ja konfidentsiaalsus;
- teises järjekorras käideldavus, terviklus ja usaldatavus.

1.4 Suunise eesmärk

1.4.1 Süsteemide keerukuse pideva kasvu ja sellele vastavate keerukate küberohtude tõttu toetuvad organisatsioonid üha enam kutseliste spetsialistide poole, kellel on süsteemide riskide ja nõrkuste leevendamiseks vajalikud tõendatud oskused, asjatundmine ja teadmised. IS audiitorid mängivad olulist rolli kiiresti muutuvale infotehnoloogiale ning sellega seotud nõrkustele ja potentsiaalsele riskiavatusele reageerimisel organisatsiooni varade kaitsmiseks, aidates tuvastada, hinnata ja leevendada riske. IS audiitorid annavad nii välisele kui ka sisemisele audititalitusele tehnilisi IT-oskusi ja asjatundmist; tehnoloogilise keerukuse kasvu tõttu rahandus- ja käituskeskkonnas kasvab aga üha enam vajadus hoida IT-alase asjatundmise oskused ja teadmised adekvaatsel tasemel. Praegusel ajastul, mil tehnoloogia on esmane äritegevuse tõukejõud või äriprotsesse toetav keskne võimaldaja, toetuvad organisatsioonid ja nende huvirühmad IS audiitorile, et otsustada, kas juhtkond on pühendunud tagama varade kaitset, andmete terviklust, toimivust ja tõhusust, üleorganisatsiooniliste poliitikate järgimist ning õiguslike, regulatiivsete ja põhikirjaliste kohustuste täitmist.

1.4.2 ISACA IS auditeerimise standardid ja COBIT rõhutavad selgelt, et audititalituse põhikiri peaks täpselt kehtestama IS audiitorite kohustused, õigused ja vastutuse auditite läbiviimiseks.

1.4.3 Just selles kontekstis on olemas vajadus suunise järele, mis annaks IS audiitoritele juhiseid nende kohustuste, õiguste ja vastutuse kohta auditiülesandeid täitma nõustumisel.

1.4.4 See suunis annab juhiseid IS auditeerimise standardite S1 "Audititalituse põhikiri" ja S3 "Kutse-eetika ja standardid" rakendamiseks. IS audiitor peaks seda suunist arvestama otsustamisel, kuidas saavutada nimetatud standardite rakendamine, kasutama suunise rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama kõiki lahknevusi.

1.5 Suunise rakendamine

1.5.1 Selle suunise rakendamisel peaks IS audiitor arvestama ta juhiseid seostatult muude asjassepuutuvate ISACA standardite ja suunistega.

G34 Kohustused, õigused ja vastutus (jätkub)

2 KOHUSTUSED

2.1 Elukutse suhtes

2.1.1 Suhtumises oma kutsetöösse peaks IS audiitor olema otsekohene, aus ja siiras.

2.1.2 IS audiitor peaks oma hoiakult ja ilmelt olema auditeeritavast sõltumatu.

2.1.3 IS audiitor peaks järgima kutse-eetika koodekseid, mida kirjutavad ette tema kutsealakogud, näiteks ISACA kutse-eetika koodeksit.

2.1.4 IS audiitor peaks sooritama oma tegevusi vastavalt kohaldatavatele auditeerimisstandarditele ning üldtunnustatud auditeerimistavadele, mis on kohaldatavad IS auditeerimise kutsealal, näiteks ISACA IS auditeerimise standarditele, suunistele ja protseduuridele.

2.1.5 Kui vastavus ei ole auditi keskkonna tingimuste tõttu saavutatav, peaks IS audiitor avaldama auditi aruandes sellise kohaldatavatest auditeerimisstandarditest lahknemise fakti, teatades ka lahknevuse põhjuse ning lahknevuse mõju auditile.

2.1.6 IS audiitor peaks alati hoidma ülal oma kutseala väärikust.

2.1.7 IS audiitor peaks järgima kohaldatavaid eeskirjade ja põhikirja nõudeid.

2.1.8 IS audiitoril peaksid olema vastuvõetud ülesannete täitmiseks vajalikud teadmised, pädevus ja oskused.

2.1.9 IS audiitor peaks sooritama kogu IS auditile määratud auditipersonali järelevalvet, tagama kvaliteeti, järgima kohaldatavaid standardeid ja soodustama personali arengut.

2.1.10 IS audiitor peaks oma järelduste ja soovituste toeks hankima ja säilitama piisavad ja pädevad auditi asitõendid. Infosüsteemide keskkonna auditeerimisel võib osa auditi asitõenditest olla elektroonilisel kujul. IS audiitor peaks andma mõistliku kinnituse sellele, et niisugused auditi asitõendid talletatakse adekvaatselt ja et vajadusel on nad tervikuna kättesaadavad.

2.2 Auditeeritava (organisatsiooni) suhtes

2.2.1 IS audiitor peaks tunnustama, mõistma ja kõikjal arvestama auditeeritava ärieesmärke, sihte ja missiooni.

2.2.2 IS audiitor peaks tundma auditeeritava kutsealaseid vajadusi IS audiitori järele, sealhulgas kõiki sõltumatuid nõudeid auditeeritavale.

2.2.3 Võimaluse ja vajaduse korral peaksid IS audiitor ja auditeeritav omavahel leppima kokku auditiülesande käsitlusala, eesmärkide ja lähtetingimuste asjus.

2.2.4 IS audiitor peaks sisejuhtimise keskkonna sobivuse hindamiseks piisavalt tundma õppima juhtkonna hoiakuid, teadlikkust ja ettevõtmisi sisemeetmete ja nende tähtsuse suhtes.

2.2.5 IS audiitor peaks sooritama läbivaadatavasse tegevusse puutuva juhtimisriski eelkaalutlemise. Auditi eesmärgid peaksid kajastama selle kaalutlemise tulemusi. IS audiitor peaks dokumenteerima auditi töödokumentides organisatsiooni juhtimissüsteemidest saadud ettekujutuse ning juhtimisriski kaalutlemise.

G34 Kohustused, õigused ja vastutus (jätkub)

2.2.6 Auditi üldise plaani koostamisel peaks IS audiitor kasutama sobivaid riski kaalutlemise meetodeid. Kui juhtimisrisk kaalutletakse madalamal tasemel, peaks IS audiitor dokumenteerima ka oma järelduste aluse. Sellisel juhul peaks IS audiitor juhtimisriski kaalutlemise toeks hankima auditi asitõendeid meetmete kontrollimise teel. Mida madalamal toimub juhtimisriski hindamine, seda rohkem peaks IS audiitor koguma auditi asitõendeid selle kohta, et infosüsteemid ja sisejuhtimise süsteemid on sobivalt kavandatud ja toimivad.

2.2.7 Meetmete kontrollimise tulemuste põhjal peaks IS audiitor otsustama, kas sisemeetmed on kavandatud nii ja töötavad nii, nagu eeldati juhtimisriski eelkaalutlemisel. Olemusliku riski ja juhtimisriski kaalutletud tasemeid peaks IS audiitor arvestama otsustamisel, millised peavad olema iseloomult, ajastuselt ja ulatuselt need sõltumatud protseduurid, mida vajatakse auditi riski vähendamiseks mingi vastuvõetava madala tasemeni.

2.2.8 IS audiitor peaks kinnitama juhtimisriski kaalutlust sõltumatute protseduuride tulemuste ning muude auditi läbiviimise ajal saadud auditi asitõendite põhjal. Kui ilmneb lahknevusi ettekirjutatud juhtimissüsteemidest, paeks IS audiitor nende tagajärgede arvestamiseks korraldama eraldi uuringuid. Kui IS audiitor niisuguste uuringute põhjal teeb järeldab, et lahknevused ei toeta juhtimisriski eelkaalutluse tulemusi, peaks ta neid tulemusi korrigeerima, välja arvatud juhul, kui muudest meetmete kontrollimistest saadud auditi asitõendid toetavad kaalutluse tulemusi. Kui IS audiitor teeb järelduse, et juhtimisriski kaalutletud tase tuleb läbi vaadata, peaks ta muutma oma plaanitud sõltumatute protseduuride iseloomu, ajastust ja ulatust.

2.2.9 IS audiitor peaks audititalituse juhtkonnaga läbi arutama ja kokku leppima ülesande auditi plaani, auditi metoodika, ressursid, ajapiirid ja aruandluse nõuded. Auditi selliste osade plaanimisel, mida võib mõjutada IS-keskkond, peaks IS audiitor saama ettekujutuse IS-tegevuste tähtsusest ja keerukusest, teatatud meetmete sobivusest ning andmete kättesaadavusest ja usaldatavusest nende kasutamiseks auditis. Selline ettekujutus hõlmab alljärgnevaid aspekte.

- Infosüsteemide infrastruktuur (riistvara, operatsioonisüsteemid ja rakendustarkvara, mida kasutab organisatsioon, sealhulgas kõik pärast viimast auditit toimunud muudatused).
- Töötluse tähtsus ja keerukus igas olulises rakenduses.
- Organisatsiooni IS-tegevuste organisatsioonilise struktuuri määramine ning töötluse keskendamise või hajutamise ulatus organisatsiooni piires, eriti, kui need võivad mõjutada kohustuste lahusust.
- Andmete kättesaadavuse määramine, kasutadaolevate andmete, lähtedokumentide ja failide usaldatavus ning muud auditi asitõendid, mida IS audiitor võib vajada ja mis võivad eksisteerida ainult lühiajaliselt või ainult masinloetaval kujul. Arvutipõhised infosüsteemid võivad genereerida aruandeid, millest võib olla kasu sõltumatute kontrollimiste (eriti analüütiliste protseduuride) sooritamisel.

2.2.10 IS audiitor peaks auditi läbi viima asjakohase hoolikuse ja kutsealase nõuetekohasusega.

G34 Kohustused, õigused ja vastutus (jätkub)

2.2.11 IS audiitor peaks talle määratud töö sooritamiseks tundma keskseid infotehnoloogia riske ja meetmeid ning kasutadaolevat tehnoloogiat, näiteks arvutipõhiseid auditeerimisvahendeid ja muid andmeanalüüsi meetodeid. Auditid tuleks sooritada pädevalt ja asjakohase kutsealase hoolikusega. Auditirühmal peaksid kollektiivselt olema (või ta peaks omandama) ta kohustuste täitmiseks vajalikud teadmised, oskused ja muud pädevused.

2.2.12 IS audiitorile ilmnenud kaalukad nõrkused sisemiste juhtimissüsteemide lahenduses või talitluses peaks audiitor tegema juhtkonna sobivale vastutustasemele teatavaks niipea kui see on praktiline.

2.2.13 Kui IS audiitori arvates on kõrgem juhtkond aktsepteerinud sellise suurusega jääkriski, mis võib olla organisatsioonile vastuvõtmatu, peaks audiitor seda küsimust arutama kõrgema juhtkonnaga. Kui jääkriski küsimus jääb lahendamata, peaks IS audiitor kaaluma selle teatamisest juhatusele, otsustamiseks.

2.2.14 IS audiitor peaks respekteerima oma töö käigus saadud teabe konfidentsiaalsust ega tohiks erivolituseta avaldada sellist teavet kolmandale poolele, kui tal ei ole selle avaldamiseks õiguslikku või kutsealast kohustust. Konfidentsiaalsuse kohustus jätkub ka pärast ülesande täitmise lõpetamist ja/või audiitori ja auditeeritava vahelise suhte lõpetamist.

2.2.15 IS audiitor peaks hoidma käigus sobivat suhtluskanalit enda ja auditeeritava vahel. Teabesuhtlus peaks olema täpne, objektiivne, selge, sisutihe, konstruktiivne, täielik ja õigeaegne.

2.2.16 Auditi lõpetamisel peaks IS audiitor esitama sobivas vormis aruande. Aruanne peaks teatama võimalikud kitsendused levitamise ja tulemuste kasutamise kohta. Aruanne peaks nimetama organisatsiooni, eeldatavad adressaadid ja kõik levitamise kitsendused. IS audiitor peaks järgima oma auditiorganisatsioonide aruandlusstandardeid, -poliitikaid ja -protseduure

2.2.17 IS audiitor peaks alati olema hoiakult ja ilmelt sõltumatu auditeeritavast. IS audiitori roll on auditeerida organisatsiooni IS- ja/või sisepoliitikaid, -tavasid ja -protseduure eesmärgiga tagada meetmete adekvaatsus organisatsiooni missiooni saavutamiseks. IS audiitor võib küll olla auditeeritava organisatsiooni üks osa, kuid tähtis ja vajalik on säilitada IS audiitori sõltumatus.

2.2.18 Kui IS audiitor on organisatsiooni juhtimisstruktuuri üks osa, peaks ta andma mõistliku kinnituse sellele, et ta ei kuulu sellesse töörühma, kelle kohus on teostada läbivaadatavas organisatsioonis teatavad IS või sisejuhtimise protseduurid.

2.2.19 Vajadusel peaks IS audiitor sooritama järeltoimingud vastavalt ülesande tingimuste nõuetele. Kui vaja, peaks IS audiitor looma ka järeltoimingute protsessi, millega seirata ja otsustada, kas juhtkonna meetmed on toimivalt teostatud või kas kõrgem juhtkond on aktsepteerinud meetmete rakendamata jätmisest tuleneva riski.

G34 Kohustused, õigused ja vastutus (jätkub)

2.3 Huvirühmade suhtes

2.3.1 IS audiitor peaks teenima huvirühmade huve seaduslikult ja ausalt, järgides kõrgeid käitumis- ja hoiakunorme ning osalemata elukutset diskrediteerivates toimingute.

2.3.2 IS audiitor peaks tooma nähtavale kõik kaalukad juhtumid või sündmused, millel on otsene seos huvirühmade huvidega.

2.3.3 IS audiitor peaks vastavalt ülesande käsitlusalale ja eesmärkidele tooma esile auditeeritava ala tegeliku ja õige asjade seisu.

2.3.4 IS audiitor peaks aruandes vältima vääri ja/või mitmemõttelisi lausungeid või selliseid lausungeid, mida võidakse tõlgendada mitmeti.

2.3.5 Kui auditi läbiviimisel oli sõltumatuse kaotuse juhtumeid, peaks IS audiitor tooma need esile.

2.4 Põhikirja ja eeskirjade suhtes

2.4.1 IS audiitor peaks hoidma end kursis kohaldatavate õigusaktide ja eeskirjadega.

2.4.2 IS audiitor peaks kontrollima vastavust kohaldatavatele põhikirja nõuetele, õigusaktidele, eeskirjadele ja lepingutele ning vajadusel otsima õigusabi.

2.4.3 IS audiitor peaks avalikustama teavet vastavalt õigusnormidele ning vajaduse korral auditeeritava nõusolekul.

2.4.4 Auditiülesannete täitmisel peaks IS audiitor kasutama litsentsitud vahendeid ja tarkvara.

2.5 Ühiskonna suhtes

2.5.1 IS audiitor peaks aitama koolitada üldsust ja auditeeritavaid, täiendades nende teadmisi infoturbe, juhtimise, riskide kaalutlemise ja käsitluse, infovarade kaitse jms alal.

2.5.2 IS audiitor peaks aitama koolitada üldsust ja auditeeritavaid tehnoloogia kasutusviiside ja võimalike kuritarvituste, juhtimismudelite, juhtimiseesmärkide, üldtunnustatud juhtimistavade, seire ja tagamise metoodikate alal.

2.5.3 IS audiitor peaks aitama koolitada üldsust ja auditeeritavaid vajalike ettevaatusabinõude ja mõeldavate vältimismeetmete alal niisugusteks juhtudeks, kus tehingud toimuvad tehnika abil.

3 ÕIGUSED

3.1 IS audiitorite õigused

3.1.1 IS audiitoril on õigus saada töövõtukiri või audititalituse põhikiri, mis spetsifitseerib auditi käsitlusala, eesmärgi ja lähtetingimused.

G34 Kohustused, õigused ja vastutus (jätkub)

3.1.2 IS audiitoril on õigus juurde pääseda asjakohasele teabele ja ressurssidele, mis on vajalikud auditi toimivaks ja tõhusaks sooritamiseks.

3.1.3 Kui IS audiitori sooritatud kontrollimine ja hindamine ei tõenda vastupidist, on IS audiitoril õigus uskuda, et juhtkond on kehtestanud sobivad meetmed pettuse vältimiseks, tõrjeks ja avastamiseks.

3.1.4 IS audiitoril on õigus taotleda selliseid andmeid ja seletusi, mis osutuvad vajalikeks ja sobivaiks võimaldama auditi objektiivset sooritamist.

3.1.5 IS audiitoril on õigus säilitada auditi käigus hangitud tööfaile, dokumente, auditi asitõendeid jms oma järelduste toena ning kasutada neid võimalike probleemide või vasturääkivuste korral alusmaterjalina.

3.2 Kitsendused

3.2.1 IS audiitoril peaksid olema piisavad teadmised pettuse tunnuste tuvastamiseks, kuid temalt ei saa oodata sellise isiku asjatundmist, kelle esmane kohus on pettuse avastamine ja uurimine.

3.2.2 IS audiitor peaks rakendama asjakohast kutsealast hoolikust ja oskuslikkust, mida võib oodata arukalt ja pädevalt spetsialistilt. Asjakohane kutsealane hoolikus ei tähenda aga eksimatust.

3.2.3 IS audiitor peaks olema valvas oluliste riskide suhtes, mis võiksid mõjutada eesmärke, tegutsemist või ressursse. Ainult kinnituse saamise protseduurid, isegi kui neid sooritatakse asjakohase kutsealase hoolikusega, ei taga kõigi oluliste riskide tuvastamist.

3.2.4 Kui IS audiitor ei ole võimeline saama vajalikku teavet, ta juurdepääs ressurssidele on kitsendatud või kui miski muu takistab tal oma ülesannete täitmist, peaks ta pöörduma oma probleemide lahendamiseks sobivate juhtkonna kõrgemate tasemete poole. IS audiitor peaks auditi läbi viima professionaalselt.

3.2.5 Kui IS audiitor on kasutanud välise asjatundja teenuseid, peaks ta hindama sellise välise asjatundja tehtud töö kasulikkust ja piisavust ning sooritama ka sobiva kontrollimise, mis kinnitaks välise asjatundja leide.

3.2.6 IS audiitor ei vastuta parandusmeetmete rakendamise eest.

4 VASTUTUS

4.1 Kutsealane vastutus

4.1.1 Traditsiooniline käsitus ja harilikud arusaamad tõlgendavad vastutust kui väärtegude hukkamõistmise ja nende eest karistamise protsessi. Kutsealaselt tuleks aga vastutuses näha positiivset stiimulit, võimalust näidata oma saavutusi ja hooldevõimet. Sellest vaatepunktist on vastutus lahutamatu ja möödapääsmatu osa toimivate suhete loomisest asjade ärategemiseks ja kohustuste võtmiseks.

G34 Kohustused, õigused ja vastutus (jätkub)

4.1.2 IS audiitori täpne roll ja suhted varieeruvad eri organisatsioonide puhul ja sõltuvad ülesande iseloomust. Seetõttu on tähtis, et valitseks selgus selles, keda hõlmab ülesanne ja milline on ülesande eesmärk. Audiitori suhted kõigi oluliste osapooltega tuleks määrata koos auditeeritavaga ja dokumenteerida töövõtukirjas.

4.1.3 Üldtunnustatud põhimõtte järgi peaks IS audiitor olema objektiivne ja seega jääma organisatsiooni juhtkonnast sõltumatuks. Juhatus või juhtkond taotleb sageli tugevamat kinnitust meetmete ja muu kohta. Juhtkonna kohus on rajada adekvaatne sisejuhtimise struktuur ja hoida see käigus. Sellistes tingimustes vastutab IS audiitor esitatud aruande usutavuse eest.

4.1.4 Vastutuse saab luua asjakohase kutsealase hoolikusega, ettenägeliku lähenemisviisiga, teenuste andmise läbipaistvusega ning usutava ja õigeaegse teabe andmisega rühmale, keda see puudutab.

4.1.5 Vastutus on kohustus anda tulemusi, mis vastavad kokkulepitud ja otseselt või kaudselt väljendatud ootustele.

4.1.6 IS audiitor peaks olema asjakohaselt ettevaatlik ja hoiduma oma kutsealaase ülesande täitmise käigus kogutud teabe avaldamisest ilma organisatsiooni nõusolekuta ükskõik kellele selles organisatsioonis, kui seda ei nõua kehtivad õigusnormid. IS audiitor peaks alati pidama silmas mitmesuguseid auditeeritavale organisatsioonile kohaldatavaid õigusnormide ja põhikirja sätteid ja andma mõistliku kinnituse sellele, et neid järgitakse teabe avalikustamise osas.

4.2 Kutsealase hooletuse vältimine

4.2.1 IS audiitor ei tohiks väljendada mingit arvamust, kui ta ei ole hankinud piisavat ja pädevat teavet ning tal ei ole asjassepuutuvaid auditi asitõendeid, mis põhinevad üldtunnustatud audititavadel.

4.2.2 IS audiitor peaks teatama asjakohastele pooltele ja/või ametivõimudele kõigist protseduuride, poliitikate ja vastavusaspektide lahknevustest, mida ta märkas ülesande täitmise käigus.

4.3 Kitsendused

4.3.1 IS audiitor ei tohiks ülesandeid vastu võtta, kui tema sõltumatus on kahjustatud või tundub olevat kahjustatud. Kui näiteks IS audiitoril on auditeeritavas organisatsioonis mingi majanduslik huvi või kui ta ei ole auditeeritavast sõltumatu, ei tohiks ta ülesannet vastu võtta. Majandushuvi juhtudeks võivad olla võlgnevus organisatsioonile või oluline investeering organisatsioonis.

4.3.2 IS audiitor ei tohiks lubada ühelgi volitamata isikul või firmal täita IS auditi ülesandeid tema nimel.

4.3.3 IS audiitor ei tohiks ebaausate vahenditega taotleda kutsealast tööd ega maksta kutsealaste ülesannete saamise eest komisjoni- või vahendustasu.

G34 Kohustused, õigused ja vastutus (jätkub)

4.3.4 IS audiitor ei tohiks reklaamida oma kutsealaseid saavutusi ega teenuseid. Iseenda ja oma kutsealaste teenuste propageerimisel ei tohiks IS audiitor

- kasutada vahendeid, mis kahjustavad kutseala mainet;
- teha liialdavaid avaldusi pakutavate teenuste, oma kvalifikatsiooni või omandatud kogemuste kohta;
- halvustada teiste IS audiitorite tööd.

4.3.5 IS audiitor ei tohiks kutsealast tööd otsida ebaeetiliste vahenditega.

5 JÕUSTUMISKUUPÄEV

5.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. märtsil 2006 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

G35 Järeltoimingud

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S8 "Järeltoimingud" määrab: "Pärast leidude ja soovituste teatamist aruandes peaks IS audiitor taotlema asjakohast teavet ja hindama seda otsustamiseks, kas juhtkond on õigel ajal rakendanud asjakohaseid meetmeid."

1.2 Seos COBITiga

1.2.1 Lai juhtimiseesmärk S3 ("Saada sõltumatu kinnitus", COBIT v3) määrab: "... saada sõltumatu kinnitus organisatsioonide, klientide ja kolmandatest pooltest tarnijate vahelise usalduse ja usaldusväärsuse suurendamiseks."

1.2.2 Lai juhtimiseesmärk S4 ("Korraldada sõltumatu audit", COBIT v3) määrab: "... korraldada sõltumatu audit usalduse suurendamiseks ja parimate tavade alastest nõuannetest kasu saamiseks."

1.2.3 Detailne juhtimiseesmärk S4.8 ("Järeltoimingud", COBIT v3) määrab: "Auditi kommentaaride lahendamine jääb juhtkonna hooleks. Audiitorid peaksid taotlema asjakohast teavet eelmiste leidude, järelduste ja soovituste kohta ning hindama seda, et otsustada, kas on õigeaegselt rakendatud sobivaid meetmeid."

1.3 Toetumine COBITile

1.3.1 Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ning arvestades COBITi teabekriteeriume ja nendega seotud juhtimistavasid. Selle nõude täitmiseks on COBITist valitud ja sobitatud tõenäoliselt kõige asjakohasemad protsessid ning need on alljärgnevas liigitatud esmajärgulisteks. Valitavad ja sobitatavad protsessid ja juhtimiseesmärgid võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest.

1.3.2 Esmajärgulised

- S3 – Saada sõltumatu kinnitus (COBIT v3)
- S4 – Korraldada sõltumatu audit (COBIT v3)

1.3.3 Järeltoimingute puhul kõige asjassepuutuvamad on järgnevad teabekriteeriumid:

- esmajärjekorras toimivus, tõhusus, konfidentsiaalsus, terviklus ja vastavus;
- teises järjekorras käideldavus ja usaldatavus.

G35 Järeltoimingud (jätkub)

1.4 Suunise eesmärk

1.4.1 Selle suunise eesmärk on anda juhiseid IS audiitoritele, kes sooritavad järeltoiminguid, mis on seotud aruannetes esitatud soovituste ja auditi kommentaaridega.

1.4.2 See suunis annab juhiseid IS auditeerimise standardi S8 "Järeltoimingud" rakendamise kohta.

1.5 Suunise rakendamine

1.5.1 Selle suunise rakendamisel peaks IS audiitor arvestama ta juhiseid seostatult muude asjassepuutuvate ISACA standardite ja suunistega.

2 JÄRELTOIMINGUD

2.1 Määratlus

IS audiitorite sooritatavaid järeltoiminguid võib määratleda "protsessina, millega nad otsustavad, kuivõrd adekvaatsed, toimivad ja õigeaegsed on meetmed, mida juhtkond rakendas talle teatatud auditileidude ja -soovituste, sealhulgas väliste audiitorite ja teiste poolt teatatute suhtes." Tuleks rajada järeltoimingute protsess, mis aitaks saada mõistlikku kinnitust sellele, et iga IS audiitorite sooritatud läbivaatus annab organisatsioonile optimaalselt kasu, nõudes, et läbivaatustest tulenevad ja kokkulepitud järeldused tehtaks teoks vastavalt juhtkonna ettevõtmistele või et juhtkond tunneks ja tunnustaks riske, mis kaasnevad pakutud meetmete edasilükkamisega või rakendamata jätmisega.

2.2 Juhtkonna soovitatud meetmed

2.2.1 IS audiitori ja auditeeritava organisatsiooni vaheliste arutamiste ühe osana peaks IS audiitor vajadusel saavutama kokkuleppe auditiülesande tulemuste kohta ja tegutsemist täiustavate meetmete plaani kohta.

2.2.2 Juhtkond peaks määrama teostuse kuupäeva, mil kõik soovitatud meetmed on ellu viidud.

2.2.3 Kui juhtkonna pakutavad meetmed talle teatatud soovituste ja auditi kommentaaride rakendamiseks või muul viisil käsitlemiseks on IS audiitoriga läbi arutatud või talle teatavaks tehtud, tuleks need meetmed juhtkonna reaktsioonina märkida lõpparuandesse koos kohustuseks võetud teostuskuupäevaga.

2.2.4 Kui IS audiitor ja auditeeritav organisatsioon ei saavuta kokkulepet mingi konkreetse soovituse või auditi kommentaari kohta, võib auditisuhtlus teatada nii seisukohad kui ka lahkarvamuse põhjused. Organisatsiooni kirjalikud kommentaarid võidakse paigutada auditi aruandesse ühe lisana. Selle asemel võib organisatsiooni seisukohad esitada aruande põhitekstis või kaaskirjas. Seejärel peab kõrgem juhtkond (või auditikomisjon, kui see on olemas) otsustama, millist seisukohta toetada.

G35 Järeltoimingud (jätkub)

Kui kõrgem juhtkond (või auditikomisjon) toetab vaadeldavas küsimuses organisatsiooni seisukohta, ei tarvitse IS audiitor selle konkreetse soovituse puhul sooritada järeltoiminguid, välja arvatud juhul, kui arvatakse, et leiu olulisus ja toimetase on IS keskkonna muutus(t)e tõttu muutunud (vt jaotis 2.4.3).

2.2.5 Mõnede läbivaatuste, näiteks rakendussüsteemide teostuseelsete läbivaatuste ajal võidakse leidudest teatada projekti töörühmale ja/või juhtkonnale pidevalt, sageli probleemiteadete kujul. Sellistel juhtudel tuleks tuleks nende probleemide puhul rakendatavaid meetmeid pidevalt seirata. Kui probleemiteate soovitused on ellu viidud, võib lõpparuandesse selle soovituse juurde märkida "lõpetatud" või "teostatud". "Lõpetatud" või "teostatud" soovitustest tuleks teatada.

2.3 Järeltoimingute protseduurid

2.3.1 Järeltoimingute sooritamiseks tuleks kehtestada protseduurid ja need peaksid hõlmama alljärgnevat.

- Ajapiirid, mille raames juhtkond peaks reageerima kokkulepitud soovitustele.
- Juhtkonna reaktsiooni hindamine.
- Reaktsiooni verifitseerimine, kui seda peetakse vajalikuks (vt jaotis 2.7).
- Järeltöö, kui seda peetakse vajalikuks.
- Suhtlusprotseduur, mis laiendab lõpetamata ja puudulike reaktsioonide või meetmete käsitluse sobivate juhtkonnatasemeteni.
- Protsess, millega saada mõistlik kinnitus juhtkonna hinnangule nende riskide kohta, mis kaasnevad parandusmeetmete hilinemisega või nende rakendamata jätmisega.

2.3.2 Järeltoiminguid aitab sooritada automatiseeritud jälgimissüsteem või andmebaas.

2.3.3 Sobivate järeltoiminguprotseduuride otsustamisel tuleks võtta arvesse järgmised tegurid:

- kõik IS keskkonna muutused, mis võivad mõjutada mingi teatatud leiu olulisust;
- teatatud leiu või soovituse olulisus;
- parandusmeetme nurjumisest tuleneda võiv toime;
- teatatud probleemi kõrvaldamiseks vajaliku panuse ja kulutuse suurusaste;
- parandusmeetme keerukus;
- hõlmatav ajavahemik.

2.3.4 Kui IS audiitor töötab siseauditi keskkonnas, peaks vastutus järeltoimingute eest olema määratletud siseauditi talituse kirjalikus põhikirjas.

G35 Järeltoimingud (jätkub)

2.4 Järeltoimingute ajastus ja ajakava

2.4.1 Järeltoimingute iseloom, ajastus ja ulatus peaksid arvestama teatatud leiu olulisust ja parandusmeetmete rakendamata jätmise toimet. IS auditi järeltoimingute ajastus algse aruande suhtes on kutsealase otsustusvõime küsimus ning sõltub reast sellistest aspektidest nagu kaasnevate organisatsiooni riskide ja kulude iseloom ja suurus.

2.4.2 Suureriskilisi probleeme puudutavate kokkulepitud tulemuste järeltoimingud tuleks sooritada peatselt pärast meetmete tähtpäeva ja neid tulemusi võib seirata progresseeruvalt.

2.4.3 Kuna järeltoimingud on IS auditi protsessi lahutamatu osa, tuleks nad ajakavastada koos muude läbivaatuse sooritamiseks vajalike sammudega. Spetsiifilisi järeltoiminguid ja nende ajastust võivad mõjutada läbivaatuse tulemused ja need tuleks määrata ala juhtkonnaga nõu pidades.

2.4.4 Ühe konkreetse aruande puhul võib järeltoimingud sooritada kõigi juhtkonna reageeringute teostamise kohta, ehkki juhtkonna määratud teostamistähtajad võivad olla erinevad. Teine võimalus on sooritada juhtkonna üksikreageeringute järeltoimingud eraldi, vastavalt juhtkonnaga kokkulepitud tähtpäevale.

2.5 Järeltoimingute edasilükkamine

2.5.1 IS audiitori kohus on ajakavastada järeltoimingud ülesande täitmise ajakavade koostamise osana. Järeltoimingute ajakavastamine peaks põhinema asjassepuutuval riskil ja sellele avatusel ning ka parandusmeetmete teostuse ajastamise raskusastmel ja olulisusel.

2.5.2 Võib esineda ka juhtumeid, kus IS audiitor otsustab, et juhtkonna suuline või kirjalik vastus näitab, et juba rakendatud meetmetest piisab, kui võrrelda neid auditi leiu või soovituse suhtelise tähtsusega. Sellistel juhtudel võib verifitseerivad järeltoimingud sooritada järgmise kõnealust süsteemi või probleemi käsitleva auditiülesande osana.

2.6 Järeltoiminguvastuste vorm

2.6.1 Kõige toimivam viis saada juhtkonnalt järelvastuseid on kirjalik vastamine, sest see aitab tugevdada ja kinnitada juhtkonna vastutust järeltoimingute ja edusammude eest. Kirjalikud vastused kindlustavad ka toimingute, kohustuste ja hetkeseisu täpse protokolli. IS audiitorid võivad saada ja jäädvustada ka suulisi vastuseid ning võimaluse korral võib juhtkond neid kinnitada. Koos vastusega võidakse anda ka tõendeid meetme kohta või soovituste elluviimise kohta.

2.6.2 IS audiitor võib taotleda ja/või saada juhtkonnalt perioodilisi ajakohastusi, et hinnata juhtkonna edusamme oma kokkulepitud toimingute sooritamisel, eriti suureriskiliste probleemide ja aeganõudvate parandusmeetmete puhul.

G35 Järeltoimingud (jätkub)

2.7 Järeltoimingute iseloom ja ulatus

2.7.1 Normaaljuhul küsib IS audiitor organisatsioonilt järeltoimingute seisu peagi pärast mõne meetme või kõigi kokkulepitud meetmete teostamiseks pakutud tähtaja möödumist. Selleks tuleb võib-olla lõpparuanne ümber vormistada, et anda organisatsioonile aruandes koht, kus dokumenteerida soovituste elluviimiseks rakendatud meetmete üksikasju.

2.7.2 Harilikult antakse organisatsioonile mingid ajapiirid, mille raames ta teatab soovituste elluviimiseks rakendatud meetmete üksikasjad.

2.7.3 Rakendatud meetmeid detailiseerivat juhtkonna vastust peaks võimaluse korral hindama see audiitor, kes sooritas algse läbivaatuse. Võimalusel tuleks rakendatud meetmete kohta alati hankida auditi asitõendeid. Näiteks võidi dokumenteerida protseduurid või koostada teatavad juhtkonna aruanded.

2.7.4 Kui juhtkond annab teavet soovituste elluviimiseks rakendatud meetmete kohta ja IS audiitoril on kahtlusi saadud teabe suhtes või rakendatud meetmete toimivuse suhtes, tuleks enne järeltoimingute lõpetamist läbi viia sobiv testimine või muu auditiprotseduur, mis tõendaks õiget seisukohta või tegelikku olukorda.

2.7.5 Järeltoimingute sooritamisel peaks IS audiitor hindama seda, kas käsitlemata jäänud leiud on endiselt relevantsed või kas nende tähtsus on kasvanud. IS audiitor võib otsustada, et mingi soovituse rakendamine ei ole enam sobiv. See võib toimuda siis, kui rakendussüsteemid on muutunud, on rakendatud korvavaid meetmeid või ärieesmärgid või prioriteedid on muutunud nii, et algne risk on kõrvaldatud või seda on tunduvalt vähendatud. IS keskkonnas toimunud muutus võib aga ka suurendada varasema leiu toimet ja ta käsitluse vajadust.

2.7.6 Järeltoimingute ülesande võib ajakavastada nii, et sellega kontrollitakse elutähtsate või oluliste meetmete teostamist.

2.7.7 IS audiitori arvamus, et juhtkonna reageeringud või meetmed on puudulikud, tuleks teha teatavaks asjakohasele juhtkonna tasemele.

2.8 Juhtkonnapoolne riskide aktsepteerimine

2.8.1 Juhtkonnakohus on otsustada sobivad meetmed, mida tuleb rakendada vastuseks talle teatatud auditi leidudele ja soovitustele. IS audiitori kohus on hinnata juhtkonna selliste meetmete sobivust ning auditi leidude ja soovitustena teatatud küsimuste lahendamise õigeaegsust.

2.8.2 Kõrgem juhtkond võib kulude tõttu või muudel kaalutlustel otsustada aktsepteerida talle teatatud olukorra parandamata jätmise riski. Kõrgema juhtkonna otsusest kõigi oluliste auditi leidude ja soovituste kohta tuleks informeerida juhatust (või auditikomisjoni, kui see on olemas).

2.8.3 Kui IS audiitor arvab, et organisatsioon on aktsepteerinud jääkriski sellise suuruse, mis ei sobi organisatsioonile, peaks ta arutama seda küsimust siseauditi talitusega ja kõrgema juhtkonnaga. Kui IS audiitor ei nõustu jääkriski puudutava otsusega, peaksid IS audiitor ja kõrgem juhtkond lahenduse saamiseks teatama sellest probleemist juhatusele (või auditikomisjoni, kui see on olemas).

G35 Järeltoimingud (jätkub)

2.9 IS siseaudiitori sooritatavad välisauditi järeltoimingud

2.9.1 Järeltoimingute kohustused jätkuvate siseauditi tegevuste puhuks tuleks määrata IS siseauditi talituse põhikirjas, muude auditiülesannete puhuks aga töövõtukirjades.

2.9.2 Sõltuvalt ülesande käsitlusalast ja tingimustest ning kooskõlas asjassepuutuvate IS auditeerimise standarditega võivad IS välisaudiitorid oma kokkulepitud soovituste järeltoimingute osas toetuda IS siseauditi talitusele.

3 KONSULTEERIMINE

3.1 Konsulteerimise tüüpi ülesanded

3.1.1 Konsulteerimistüüpi ülesandeid või teenuseid võib määratleda nii: "nõustavad ja nendega seotud klienditeenindustegevused, mille iseloom ja käsitlusala lepitakse kokku kliendiga ning mis on mõeldud lisama väärtust organisatsiooni tegutsemisele ja täiustama seda. Näiteid: nõustamine, teabeabi, edendamine, protsesside kavandamine, koolitus."[2] Ülesande iseloom ja käsitlusala tuleks kokku leppida enne ülesandega alustamist.

3.1.2 IS audiitor peaks konsulteerimisülesannete tulemusi organisatsiooniga kokkulepitud ulatuses seirama. Konsulteerimisülesannete eri tüüpidele võivad sobida erinevad seire tüübid. Seire töömaht võib sõltuda sellistest teguritest nagu juhtkonna ilmutatav huvi ülesande tulemuste vastu, projekti riskide hinnang IS audiitorilt, ülesande täitmisel väljaselgitatud potentsiaalne lisandväärtus organisatsioonile.

4 ARUANDLUS

4.1 Järeltoimingute aruandlus

4.1.1 Auditikomisjonile (kui see on moodustatud) või organisatsiooni juhtkonna sobivale tasemele tuleks esitada aruanne IS auditiaruannetest tulenevate kokkulepitud parandusmeetmete seisu kohta, näidates selles ka kokkulepitud, kuid teostamata soovitused.

4.1.2 Kui IS audiitor leiab järgneva ülesande täitmisel, et mingi meede, mis juhtkonna väitel olevat rakendatud, tegelikult aga mitte, peaks ta sellest teatama kõrgemale juhtkonnale ja auditikomisjonile (kui see on olemas).

4.1.3 Kui kõik parandusmeetmed on teostatud, võib kõrgemale juhtkonnale (või auditikomisjonile, kui see on olemas) edastada aruande, mis detailiseerib kõiki teostatud või lõpetatud meetmeid.

5 JÕUSTUMISKUUPÄEV

5.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. märtsil 2006 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

[2] Siseauditeerimise kutsealaste tavade rahvusvahelised standardid. Sõnastik. IIA.

G36 Biomeetrilised meetmed

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "IS auditi personalile tuleks rakendada järelevalve mõistliku kinnituse saamiseks sellele, et auditi eesmärgid saavutatakse ja kohaldatavaid kutsealaseid auditeerimisstandardeid järgitakse. Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite sobiva analüüsi ja tõlgendamisega."

1.1.2 Standard S10 "IT ohje" määrab: "IS audiitor peaks IS talituse läbi vaatama ja otsustama, kas see talitus on kooskõlas organisatsiooni missiooni, visiooni, väärtuste, eesmärkide ja strateegiatega... IS audiitor peaks läbi vaatama IS ressursi- ja sooritusehalduse protsesside toimivuse ja seda hindama."

1.2 Seos COBITiga

1.2.1 Juhtimisprotsess HE1 "Tuvastada automatiseeritud lahendused" määrab: "Tegevusalast nõuet IT-le – muundada ettevõtte talitluslikud ja juhtimisnõuded automatiseeritud lahenduste toimivaks ja tõhusaks kavandiks – rahuldava ning tehniliselt teostatavate ja kuluefektiivsete lahenduste leidmisele keskendatud IT-protsessi (automatiseeritud lahenduste tuvastamise) juhtimine saavutatakse sellega, et

- määratletakse tegevusalased ja tehnilised nõuded;
- sooritatakse teostuvusuuringud, nii nagu on määratletud arendusstandardites;
- kinnitatakse nõuded ja teostuvusuuringu tulemused (või lükatakse need tagasi);

ning protsessi mõõtmise näitajad on

- nende projektide arv, kus väärade teostuvuseelduste tõttu ei saavutatud sõnastatud tulemusi;
- talitlusprotsessi omaniku poolt kinnitatud teostuvusuuringute protsent;
- pakutavate funktsioonidega rahuldatud kasutajate protsent."

1.2.2 Juhtimisprotsess HE3 "Hankida tehnoloogia infrastruktuur ja hooldada seda" määrab: "Tegevusalast nõuet IT-le – hankida integreeritud ja standardne IT infrastruktuur ja hooldada seda – rahuldava ning tegevusalaste rakenduste jaoks sobivate platvormide loomisele kooskõlas määratletud IT arhitektuuriga ja tehnoloogia standarditega keskendatud IT-protsessi (tehnoloogia infrastruktuuri hankimise ja hooldamise) juhtimine saavutatakse sellega, et

- koostatakse tehnoloogia hankimise plaan, mis on kooskõlas tehnoloogia infrastruktuuri plaaniga;
- plaanitakse infrastruktuuri hooldus;
- rakendatakse sisejuhtimise, turbe ja auditeerimise meetmeid;

ning protsessi mõõtmise näitajad on

- nende platvormide protsent, mis ei ole kooskõlas määratletud IT-arhitektuuriga ja tehnoloogia standarditega;
- vananenud (või kiiresti vananeva) infrastruktuuriga toetatavate elutähtsate talitlusprotsesside arv;
- enam mitte (või peagi enam mitte) toetatavate infrastruktuurikomponentide arv."

1.2.3 Juhtimisprotsess HE5 " Hankida IT-ressursid " määrab: "Tegevusalast nõuet IT-le – suurendada IT kuluefektiivsust ja IT panust tegevuse kasumlikkusse – rahuldava ning tarnestrateegiale vastavate IT-oskuste omandamisele ja säilitamisele, integreeritud ja standardsele IT infrastruktuurile ja IT soetamise riskile keskendatud IT-protsessi (IT-ressursside soetamise) juhtimine saavutatakse sellega, et

- konsulteeritakse õigus- ja lepingualaste küsimistes;
- määratletakse soetamise protseduurid ja standardid;
- soetatakse taotletav riistvara, tarkvara ja teenused kooskõlas määratletud protseduuridega;

ning protsessi mõõtmise näitajad on

- soetamislepingutega seotud vaidluste arv;
- soetamiskulude vähenemine;
- tarnijatega rahul olevate oluliste huvipoolte protsent;
- platvormide protsent."

1.2.4 Juhtimiseesmärk HE3.1 määrab: "Koostada kehtestatud tegevusalastele talitluslikele ja tehnilistele nõuetele vastava ja organisatsiooni tehnoloogiasuunaga kooskõlas oleva infrastruktuuri hankimise, evituse ja hooldamise plaan. Plaan peaks olema paindlik ja arvestama tulevasi suutvuse lisamisi, siirdekulusid, tehnilisi riske ja investeeringu eluiga tehnoloogia ajakohastamiste puhul. Uue tehnilise võime lisamisel hinnata keerukuskulusid ning tarnija ja toote ärilist elujõudu."

1.3 Toetumine COBITile

1.3.1 Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ning COBITi juhtimiseesmärkide ja nendega seotud juhtimistavade arvestamisel.

1.3.2 Protsessid ja juhtimiseesmärgid, mis tuleb valida ja kohaldada, võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest. Nõuete täitmiseks on valitavad ja kohaldatavad COBITi protsessid, mis on kõige tõenäolisemalt asjakohased, alljärgnevas loetelus jagatud esmasteks ja teisesteks.

1.3.3 Esmajärjekorras

- PO1 – Määratleda strateegiline IT plaan
- PO3 – Määrata tehnoloogiline suund

- PO5 – Hallata IT-investeeringuid
- PO8 – Hallata kvaliteeti
- PO9 – Hinnata IT riskid ja hallata neid
- PO10 – Hallata projekte
- HE1 – Tuvastada automatiseeritud lahendused
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE5 – Hankida IT-ressursid
- TT1 – Määratleda teenusetasemed ja hallata neid
- TT3 – Hallata suutlikkust ja võimsust
- TT4 – Tagada pidev teenus
- TT5 – Tagada süsteemide turvalisus
- TT7 – Koolitada kasutajaid
- SH1 – Seirata ja hinnata IT töötulemusi
- SH2 – Seirata ja hinnata sisejuhtimist
- SH3 – Tagada vastavus välisnõuetele

1.3.4 Teises järjekorras

- PO6 – Teavitada juhtimissihid ja suund
- HE6 – Hallata muutusi
- TT9 – Hallata konfiguratsiooni
- TT10 – Hallata probleeme
- TT11 – Hallata andmeid

1.3.5 Biomeetriliste meetmete puhul on kõige asjakohasemad teabekriteeriumid

- esmajärjekorras: toimivus, tõhusus ja käideldavus;
- teises järjekorras: konfidentsiaalsus, terviklus ja usaldatavus.

1.4 Suunise eesmärk

1.4.1 Traditsioonilised identifitseerimise ja autentimise – pääsu reguleerimise nurgakivide – vahendid põhinevad "millelgi, mida te teate" (näiteks PIN-kood või parool) ja "millelgi, mis teil on" (näiteks kiipkaardid või automaadikaardid). Nende meetodite puhul tuleb sõltuda oma mälust (et pidada meeles parooli või kanda kaasas kaarti), kuid peale selle ei erista kumbki neist isikut üheselt. Paroolidel ja pääsmikupõhistel süsteemidel on oma puudused ja sageli tekitavad nad kitsaskohti, eriti kriisiolukorras. Tehnoloogia areng tekitas paradigma nihke usaldatavamate pääsu reguleerimise vahendite, "millegi, mis te olete", st biomeetriapõhiste pääsu reguleerimise meetmete poole.

1.4.2 Biomeetrilise pääsu reguleerimise süsteemi väga oluline näitaja on täpsus. Harilikult on identifitseerimine isiku tunnusomaduste üks-mitmest-otsing talletatavate kujutiste andmebaasist, autentimine on aga üks-ühest-otsing isiku väidetava identiteedi tõendamiseks. Harilikult rakendatakse biomeetrilist tunnust identifitseerimiseks füüsilise pääsu reguleerimise mehhanismides ja autentimiseks loogilise pääsu reguleerimise mehhanismides. Süsteem eksib, kui ta ei suuda eristada autentset isikut selle teesklejast. On tähtis, et väära keeldumise (väära eituse) ja väära aktsepteerimise (väära jaatuse) juhtumeid oleks vähe ja et nende sagedus oleks selline, mida organisatsioon peab kulude ja riski kaalutlemise tulemuse põhjal vastuvõetavaks.

1.4.3 Biomeetrilist tehnoloogiat sisaldava turbearhitektuuri üha laiema leviku tõttu on IS audiitorile saanud möödapääsmatuks olla teadlik selle tehnoloogiaga seotud riskidest ja vastumeetmetest. Talitluslike eesmärkide saavutatuses veendumiseks peaks biomeetriliste meetmete süsteemi läbivaatav IS audiitor hästi tundma seda tehnoloogiat, talitlusprotsessi ja juhtimiseesmärki

1.4.4 Selles kontekstis on vaja suunist, millega anda juhiseid IS audiitoritele, kes auditiülesannete täitmisel vaatavad läbi biomeetrilisi meetmeid.

1.5 Suunise rakendamine

1.5.1 See suunis annab juhiseid IS auditeerimise standardi S6 "Audititöö sooritamine" ja standardi S10 "IT ohje" rakendamiseks.

1.5.2 . IS audiitor peaks arvestama seda suunist, kui ta otsustab, kuidas saavutada vastavus ülalnimetatud standarditele, kasutama selle rakendamisel kutsealast otsustusvõimet ja olema valmis põhjendama kõiki lahknevusi.

1.5.3 Selle suunise rakendamisel peaks IS audiitor arvestama ta juhiseid seoses muude asjassepuutuvate ISACA standardite, suuniste ja protseduuridega.

2 BIOMEETRILISED MEETMED

2.1 Sissejuhatus

2.1.1 Sõna "biomeetria" on moodustatud kreeka sõnadest *bios* (elu) ja *metron* (mõõt). Ta on määratletud kui isiku automaatne identifitseerimine või tõendamine füsioloogiliste või käitumuslike erijoonte põhjal. Biomeetriateadus kasutab ära isiku füsioloogiliste või käitumuslike iseärasuste ainulaadsuse eelise.

2.1.2 Biomeetrilised meetmed tähendavad isiku füsioloogiliste või käitumislike erijoonte kasutamist poliitikate, protseduuride, tavade ja organisatsiooniliste struktuuride kavandamiseks eesmärgiga saada mõistlik kinnitus sellele, et identifitseerimise ja volitamisega seotud talitluslikud eesmärgid saavutatakse ning et soovimatud sündmused välditakse või avastatakse ja heastatakse.

2.1.3 Tüüpiliselt täidavad biomeetrilised süsteemid ülesandeid, mis on loetletud **joonisel 1**.

G36 Biomeetrilised meetmed (jätkub)

Joonis 1. Biomeetrilise süsteemi tüüpilised ülesanded

Registreerimine	Registreerimisprotsess nõuab, et kasutajaks taotleja annaks süsteemile biomeetrilise näidise, mis muundatakse digitaalselt ja salvestatakse hoidlasse kui võrdlusmall. Paljud biomeetrilised süsteemid kasutavad mitut näidist ja võrdlusmalli loomiseks kasutatakse kõigi mallide keskmist.
Andmete talletus	Individuaalseid võrdlusmalle talletatakse kättesaadavas hoidlas kasutaja biomeetriliste tunnuste kontrollimiseks reaalajas võtu ajal. Hoidla võib olla kohalik biomeetrilises seadmes, olla tsentraalne ja kaugemal, asuda portatiivses pääsmikus (näiteks kiipkaardis) või olla nende võimaluste kombinatsioon.
Andmehõive	Andmed hõivatakse lubatavate kasutajate identifitseerimiseks ja autentimiseks, et nad saaksid juurdepääsu. Andmed hõivatakse iga kord, kui kasutaja soovib saada juurdepääsu.
Edastus	Identifitseerimise ja autentimise otstarbeks hõivatavate andmete edastuseks kasutab süsteem sidekanalit. See kanal võib olla biomeetrilise süsteemi sees või väljaspool seda, näiteks kohtvõrk.
Signaalitöötlus	Signaalitöötlus või pilditöötlus sisaldab hõivatud andmete ja talletatavate andmete võrdlemist ja valideerimist. Hoidlas talletatavat võrdlusmalli võrreldakse hõivatud andmetega ning tulemus põhineb ühtivuse määral.
Otsustus	See on funktsioon, kus tehakse otsus ühtivuse või lahknevuse kohta, st kasutajale pääsu andmise või sellest keeldumise kohta.

2.2 Identifitseerimine ja autentimine

2.2.1 Biomeetria on automatiseeritud protsess elusa isiku identifitseerimiseks või autentimiseks ta füsioloogiliste või käitumislike erijoonte põhjal.

2.2.2 Biomeetrias sisaldab identifitseerimine isiku erijoonte üks-mitmest-otsingut andmehoidlast. Autentimine sisaldab biomeetrias üks-ühest-otsingut isiku väidetava identiteedi kontrollimiseks.

2.2.3 Tüüpiliselt kasutab biomeetria identifitseerimist füüsilise pääsu mehhanismides, autentimist aga loogilise pääsu mehhanismides.

2.3 Sooritusvõime mõõdud

2.3.1 Sooritusvõime mõõdud on mõeldud toodete hindamisel abistava etaloni saamiseks. IS audiitorid peaksid neid mõõte arvestama biomeetriliste süsteemide sooritusvõime hindamisel auditiülesande käigus. Biomeetriliste süsteemide esmased mõõdud on loetletud alljärgnevas ja esitatud **joonisel 2.**

2.3.2 Väära keeldumise sagedus (FRR) ehk I tüüpi viga – selliste juhtude protsent, kus süsteem tõrjus õige isiku.

FRR (%) = väärade keeldumiste arv × 100 / üheste katsete koguarv

2.3.3 Väära aktsepteerimise sagedus (FAR) ehk II tüüpi viga – selliste juhtude protsent, kus süsteem aktsepteeris väära isiku.

FAR (%) = väärade aktsepteerimiste arv × 100 / üheste katsete koguarv

2.3.4 Vigade ühissagedus (CER) – selliste juhtude protsent, kus FRR = FAR. Graafikul on see FAR ja FRR kõverate lõikepunkt. Vigade ühissagedus näitab süsteemi, kus on hea tasakaal tundlikkuse ja sooritusvõime vahel.

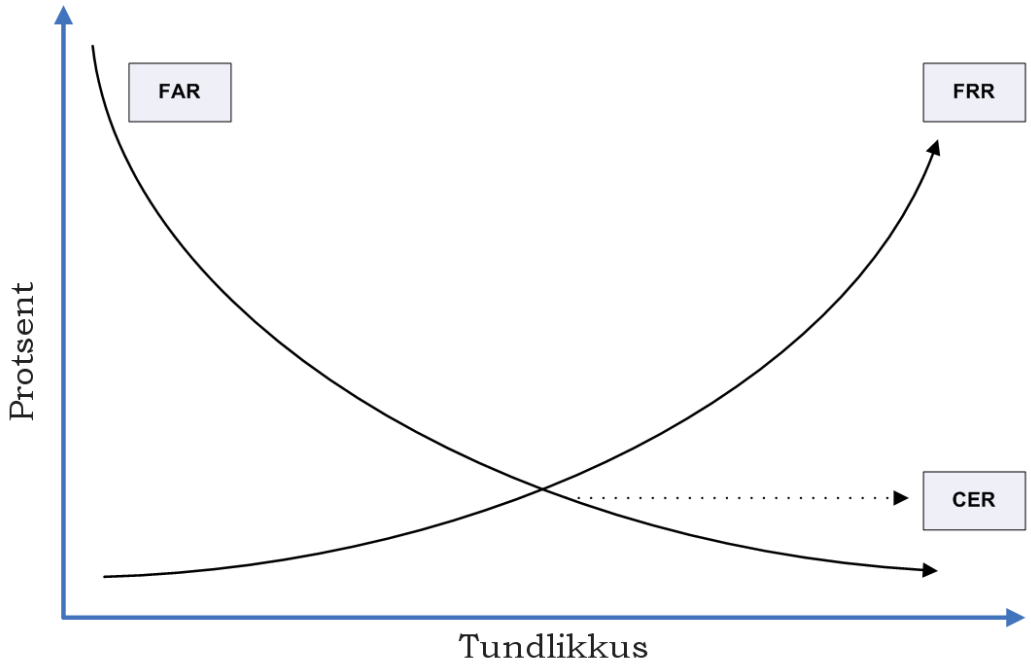
2.3.5 Registreerimisaeg – aeg, mis kulub uue isiku algseks registreerimiseks süsteemi, näidiste võtuna võrdlusmallide loomiseks.

2.3.6 Registreerimistõrgete sagedus (FTER) – näitab registreerimiskatsete nurjumise sagedust.

FTER = nurjunud registreerimiste arv / kasutajate registreerimiskatsete koguarv.

2.3.7 Läbilaskevõime – aeg, mis süsteemil kulub identifitseerimis- või autentimisfunktsiooni töötlemisel toiminguandmete valideerimiseks hoidlas olevate andmete põhjal. See on aeg, mis kulub registreeritud isikute töötlemisele süsteemipoolse aktsepteerimise või keeldumise saavutamiseks.

Joonis 2. FAR, FRR ja CER graafiku näide (illustratiivne)



Biomeetrilise süsteemi tundlikkuse kasvamisel FAR kahaneb ja FRR kasvab.

2.4 Biomeetriliste süsteemide tüübid

2.4.1 Biomeetrilised süsteemid jagunevad laias laastus kahte klassi: ühed põhinevad füsioloogilistel erijoontel (st sellel, "mis me oleme"), teised aga käitumislikel erijoontel (st sellel, "mida me teeme").

2.4.2 Mitmesugused füsioloogilistel erijoontel põhinevad biomeetrilised süsteemid on loetletud **joonisel 3**.

G36 Biomeetrilised meetmed (jätkub)

Joonis 3. Füsioloogilistel erijoontel põhinevad biomeetrilised süsteemid

Biomeetriline süsteem	Andmete registreerimine / Andmehõive
Sõrmejälg	Kujutis saadakse, kui isik surub omasõrme tugevalt vastu klaas- või polükarbonaatplaati.
Sõrmeots	Jäädvustatakse nahaalune veresoonte muster.
Sõrmelüli	Jäädvustatakse esimese ja teise liigese vaheline sõrmelüli.
Käe geomeetria	Käe ja sõrmede pikkuse, laiuse ja kõrguse ruumilise esituse saamiseks jälgitakse kaameratega korraga püst- ja rõhtkujutisi.
Silma võrkkest	Kaameraga jäädvustatakse võrkkesta veresoonte muster silma sisemuse tagaosas.
Silma vikerkest	Kaameraga jäädvustatakse vikerkesta (silmaava ümbritseva värvilise osa 9 kujutis.
Randmeveenid	Jäädvustatakse veenide muster randmel.
Sõrmeliigesekurrud	Sõrmeliigeste kurdude muster jäädvustatakse, kui isik pigistab pihuga latti.
Näo tuvastus	Näo kujutised jäädvustatakse kvaliteetkaameratega.
Näo termograafia	Näokudede soojusmustrid jäädvustatakse termotundlike seadmetega.

2.4.3 Mitmesugused käitumislikel erijoontel põhinevad biomeetrilised süsteemid on loetletud **joonisel 4.**

Joonis 4. Käitumislikel erijoontel põhinevad biomeetrilised süsteemid

Biomeetriline süsteem	Andmete registreerimine / Andmehõive
Hääle tuvastus	Hääl muundatakse digitaalselt häälejäljeks ja salvestatakse kahendarvudena.
Klahvivajutuste dünaamika	Mõõdetakse isiku hoideaega (klahvivajutuse kestus) ja siirdeaega (ühelt klahvilt teisele siirdumise kestust).
Allkirja dünaamika	Võrreldakse isiku allkirja ning jälgitakse allkirja kirjutamise kiirust, rõhku ja ajastust.

2.5 Andmete talletus

2.5.1 Võrdlusmalle tuleks hoida nende kiireks võtuks ja võrdluseks kättesaadavas hoidlas.

2.5.2 Kohalik talletus biomeetrilises lugemisseadmes võimaldab võrdlusmalle kiiresti kätte saada ja kiiremini võrrelda ning seadet paindlikumalt rakendada. Kui aga süsteemi adekvaatselt ei toeta varunduse ja taaste protsess, nõuab ta krahhi korral kordusregistreerimist.

2.5.3 Suured organisatsioonid talletavad võrdlusmalle tsentraalses hoidlas, mis võimaldab kasutajail end registreerida tsentraalsetes kohtades ja lasta end ära tunda võrkuühendatud biomeetrilistel seadmetel. Tsentraalne hoidla võimaldab varundust, taastet ja auditeeritavaid omadusi. Võtt on suhteliselt aeglasem, eriti kui andmete maht on suur.

2.5.4 Kui kasutaja kannab biomeetrilisi võrdlusnäidiseid endaga kaasas ning vastutab nende privaatsuse, konfidentsiaalsuse, käideldavuse ja tervikluse eest, tuleks võrdlus malle talletada kiipkaardis. Kiipkaartidel võib vahendi lisaturbeks olla ka täiendavaid turbefunktsioone, näiteks krüpteerimine ja digitaalallkiri.

2.5.5 Andmete konfidentsiaalsust ja terviklust tuleks hallata nii, et isikuandmed oleksid kaitstud lubamatu juurdepääsu eest.

2.6 Biomeetrilise süsteemi riskid ja turvameetmed

2.6.1 IS audiitor peaks olema teadlik biomeetrilise süsteemi tüüpilistest riskidest ja turvameetmetest. Kõige tavalisemad riskid ja vastumeetmed on loetletud **joonisel 5**.

Joonis 5. Biomeetrilise süsteemi tavalised riskid ja vastumeetmed

Riskid	Näiteid	Võimalikud vastumeetmed
Spuufimis- ja jäljendusründed	Tehissõrme kasutamine biomeetrilisel sõrmejäljeseadmel	Mitmetunnuseline biomeetria, elususe tuvastus, interaktiivne autentimine
Võltsmalli risk	Serveris talletatakse võltsmalli	Krüpteerimine, sissetungi tuvastuse süsteem (IDS), kiipkaardid
Edastusrisk	Registreerimise või andmehõive ajal püütakse edastatavad andmed kinni	Interaktiivne autentimine, identsete signaalide kõrvalejätt, süsteemi integratsioon
Mitmikkastuse risk	Sama võrdlusmalli kasutatakse eri rakendustes erinevate turvatasemetega	Räsifunktsioonid, kodeerimisalgoritmid
Komponendi muutmise risk	Kahjurkood, trooja hobune vms	Süsteemi integratsioon, turvapoliitika korralik rakendamine
Registreerimise halduse ja süsteemi kasutamise risk	Andmete muutmine registreerimise, halduse ja süsteemi kasutamise ajal	Turvapoliitika korralik rakendamine
Müra ja toitekao risk	Valguse vilkumine optilisel anduril, sõrmejälje muutuv temperatuur või niiskus	Turvapoliitika korralik rakendamine
Võimsuse ja ajastuse analüüsi risk	Biomeetrilise võrdlusmalli kohta kogutakse andmeid tarbitava võimsuse analüüsi ja diferentsiaalanalüüsiga	Mürageneraatorid, väikese võimsustarbega kiibid biomeetrilistes seadmetes
Jääktunnuse risk	Andurile jäänud sõrmejälje kopeerimine mitmesuguste meetoditega	Tehnoloogia hindamine, pääsu reguleerimine mitme vahendiga
Sarnase võrdlusmalli või sarnase erijoone risk	Ebaseadusliku kasutaja võrdlusmall sarnaneb seadusliku kasutaja omale	Tehnoloogia hindamine, pääsu reguleerimine mitme vahendiga, kalibreeringu läbivaatus

G36 Biomeetrilised meetmed (jätkub)

Jõuründe risk	Sissetungija kasutab süsteemi petmiseks jõurünnet	Konto lukustamine pärast mitut nurjunud pääsukatset
Sissesüstimise risk	Kinnipüütud digitaalsignaal süstitakse autentimissüsteemi	Edastuse turve, skanneri aktiveerimine soojusanduriga (näitab sooja keha juuresolu), ajatemplid kujutiste digitaalesitustel
Kasutajate keeldumine	Biomeetriliste meetodite pealetükkiv iseloom võib panna kasutajaid süsteemi kasutamisest loobuma	Kasutajate koolitus ja teadvustamine ning kõige vähem pealetükkivate meetodite valimine
Füüsiliste tunnuste muutumine	Mõned meetodid põhinevad näo või käe erijoontel, kuid need inimaspektid võivad aegamööda muutuda	CER seire
Muude pärandsüsteemidega integreerimise hind	Kokkusobitamine muude integreeritavates pärandsüsteemides kasutatavate meetoditega	Kulude ja tulude analüüs
Andmete kaotsimineku risk	Ketta või riistvara rike	Andmete varundus ja taaste

3 AUDITI PROTSEDUUR

3.1 Biomeetrilise süsteemi valimine ja hankimine

3.1.1 IS audiitor peaks kaaluma järgnevate biomeetrilise süsteemi valimise ja hankimisega seotud protsesside läbivaatust.

- biomeetrilise süsteemi installeerimise sihid ja nende kooskõla organisatsiooni tegevusalaste eesmärkidega;
- biomeetrilise süsteemi valimise uuring riskianalüüsi ja varade liigituse põhjal, mis arvestab ka privaatsust ja juriidilisi küsimusi;
- mõjud riskianalüüsi järgi ja leevendamise plaan;
- biomeetriliste meetmete kasutamise mõju tegevusele;
- biomeetriliste meetmete mõju töötajaile, klientidele ja partneritele;
- biomeetrilise süsteemi tasuvus võrreldes traditsiooniliste pääsu reguleerimise süsteemidega, näiteks kasutaja identifikaatoril ja paroolil põhineva autentimisega;
- biomeetrilise toote moraalne vananemine;
- toote vastavus ala standarditele ja sisemaistele või rahvusvahelistele standarditele;
- toote sooritusvõime turu-uuring ja tarnija hooldustugi;
- tarnija sertifitseeritus ja toote sertifitseeritus;
- süsteemi pealetükkivus andmete kogumisel;
- omaksvõtt kasutajate hulgas, analoogilises valdkonnas ja muudes valdkondades või muudes organisatsioonides;
- juriidilised küsimused ja kasutajate õigused (privaatsus).

G36 Biomeetrilised meetmed (jätkub)

3.2 Biomeetrilise süsteemi käitus ja hooldus

3.2.1 IS audiitor peaks kaaluma järgmiste biomeetrilise süsteemi käituse ja hooldusega seotud aspektide läbivaatust.

- Biomeetriapoliitika ja selle kooskõla organisatsiooni turvapoliitikaga.
- Biomeetrilise teabe konfidentsiaalsuse, tervikluse ja käideldavuse (CIA) kaitse, piiratud juurdepääs andmehoidlale.
- Biomeetrilise süsteemi tõhususe seire selliste andmete analüüsimise teel, nagu registreerimisaeg, õnnestumise sagedused, tõrgete sagedused, läbilaskevõime, seisuaeg, väärad jaatused, väärad eitused, keskmine tõrketu töövältus (MTBF), keskmine taasteaeg (MTTR) ja FTER.
- Biomeetrilise süsteemi liidestus muude rakenduste ja süsteemidega (näiteks, ühekordse sisselogimisega).
- Liidestus organisatsiooni teiste biomeetriliste süsteemidega.
- Käitus- ja hoolduskulude analüüs.
- Andmete salvestusmahu nõuded.
- Andmete turbe, varunduse ja taaste protseduurid.
- Versioonitäiendite ja paikade haldus.
- Kasutajakirjete hävitamine pärast töösuhte lõpetamist ettevõttes.
- Talitluse jätkuvus biomeetrilise süsteemi rikke korral ning varusüsteemide või korvavate turvamehhanismide olemasolu.
- Sobiv muutuste ohje rollipõhise pääsu kasutamisel.

3.3 Kasutajate koolitus ja omaksvõtt kasutajate hulgas

3.3.1 IS audiitor peaks kaaluma järgmiste, biomeetrilise süsteemi kasutajate koolituse ja omaksvõtuga seotud aspektide läbivaatust

- Biomeetriapoliitika teatavakstegemine organisatsioonis.
- Kohustumus turvata tegelike kasutajate biomeetrilist teavet ja privaatsust.
- Kohustumus järgida kohaldatavaid õigusnorme privaatsuse ja biomeetria alal.
- Kasutajate teadlikkus biomeetrilisest autentimissüsteemist.
- Biomeetrilise süsteemi rollide ja kohustuste piiritlemine.
- Koolitusvajaduste, koolituse ajakava, konsultatsioonipunkti ja tugiteenuse piiritlemine.
- Koolitus süsteemi kasutamise, kaitse ning süsteemi- ja eneseprofülaktika alal.
- Dokumenteeritud koolitusmaterjali ja teabesiltide olemasolu.

- Süsteemi omaksvõtt kasutajate hulgas organisatsioonis.
- Süsteemi kahjustamise või saboteerimise risk, mille tekitavad kasutajad, kellele süsteem on vastumeelne.

3.4 Süsteemi sooritusvõime

3.4.1 IS audiitor peaks kaaluma järgmiste biomeetrilise süsteemi sooritusvõimega seotud aspektide läbivaatust.

- Süsteemi liidestus rakendustega.
- Kasutajate registreerimise, ümberregistreerimise ja kõrvaldamise protsess.
- Nõuded isiku ja süsteemi kokkupuutele.
- Süsteemi testimine, verifitseerimine, valideerimine ja kinnitamine.
- Pääsu määratlemise ja administraatori privileegide testimine.
- Kaitse manipuleerimise ja saboteerimise eest.
- Kaitse andmete paljastamise eest.
- Andmete varundamine.
- Jätkusuutlikkuse plaanimine (JSP) süsteemi rikke puhuks ja JSP testimine.
- Perioodiline testimine (näiteks jõurünnete tõrjeks).
- Võltsimiskindlus ja töökindlus pikemaajalisel kasutamisel.

3.5 Rakenduste ja andmebaasi turvameetmed

3.5.1 IS audiitor peaks kaaluma järgmiste biomeetrilise süsteemi pääsumehhanismide ja konfiguratsioonisätetega seotud aspektide läbivaatust.

- Platvormi turbe konfiguratsiooni sätted, sealhulgas juurdepääsu kitsendamine isikute kogu biomeetrilisele teabele, andes pääsu ainult neile, kellel on hetkel range tööalane vajadus.
- Sissetungi tuvastuse mehhanismid.
- Tehingute turvameetmed.
- Võrgu ja kanalite krüpteerimine.
- Hoidlas talletatavate andmete krüpteerimine.
- Muudatuste haldus (tarkvaras ja riistvaras)
- Andmebaasi haldus ja hooldus.
- Riistvara ja tarkvara installeerimine.

G36 Biomeetrilised meetmed (jätkub)

3.6 Kontrolljäljed

3.6.1 IS audiitor peaks kaaluma järgmiste, biomeetrilise süsteemi kontrolljälgedega seotud aspektide läbivaatust:

- pääsulogi,
- toimingute logi,
- muutuste logi,
- pääsu blokeerimise logi,
- süsteemi seisuaja logi.

4 AUDITI KAALUTLUSI

4.1 Biomeetrilise süsteemi kasutamise ajaloolisi probleeme

4.1.1 Biomeetria kasutamise kaalumisel tuleb arvestada järgmisi probleeme.

- Privaatsuse probleemid. Teatavad terviserikked, näiteks diabeet või insult põhjustavad muudatusi võrkkesta veresoonte mustris. Võrkkestapõhist biomeetrilist süsteemi kasutav organisatsioon võib sobimatult saada terviseteavet, mida võidakse kasutada süsteemi kasutajale kahju tekitamiseks. Enne iga biomeetrilise süsteemi installeerimist tuleks arvestada kõiki õigusnorme, mis puudutavad füüsiliste erijoonte kasutamist ja hõivet.
- Andmete kogumise pealetükkivus. Kasutaja tundlikkus tema isikuruumi tungimise vastu skaneerimisel.
- Tervisekahjustuste kartus. Kartus saada nakkushaigust mingi nakatatud pinna (näiteks sõrmejäljeskanneri) kaudu.
- Süsteemi kasutamise oskus. Mõnedel kasutajatel ei ole võib-olla süsteemi kasutamiseks vajalikku oskust (st kirjaoskust või võimet) või nad võivad kahelda süsteemi tegelikus sooritusvõimes. Süsteemi sooritusvõimet võivad piirata töötingimused (näiteks määrdunud käsi, tolmused alad).
- Süsteemi stabiilsus. Biomeetriline tehnoloogia ei ole lollikindel ja peab ületama biomeetriliste rakenduste usaldatavusega seotud probleeme. Tuleb läbi vaadata väära keeldumise ja väära lubamise mõju, nii talitluse kui ka maine seisukohalt. Välistada ei saa ka oma inimeste manipulatsioone ja sabotaaži.
- Rakendamise kulud. Igas pääsupunktis biomeetriliste seadmete rakendamine võib olla kallis ja tarbida ressursse.
- Õigsus. On olemas võimalus, et volitamata kasutajad saavad juurdepääsu ja et volitatud kasutajaile pääsu ei anta.

- Vastuseis muudatustele. Võib olla juhtumeid, kus kasutajad on vastu biomeetriliste süsteemide kasutamisele.
- Kohalike õigusaktide ja põhikirja nõuded biomeetriliste süsteemide kasutamisele ning süsteemi vastuvõetavus kasutajaskonnale.

5 JÕUSTUMISKUUPÄEV

5.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. veebruaril 2007 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

Allikaviited

IT Halduse Instituut. Biomeetrilise tehnoloogia risk ja ohje. USA. 2004

G37 Konfiguratsioonihalduse protsess

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "IS auditi personalile tuleks rakendada järelevalve mõistliku kinnituse saamiseks sellele, et auditi eesmärgid saavutatakse ja kohaldatavaid kutsealaseid auditeerimisstandardeid järgitakse. Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.2 Seos COBITi versiooniga 4.1

1.2.1 Juhtimisprotsess HE2 "Hankida rakendustarkvara ja hooldada seda" määrab: "Tegevusalast nõuet IT-le – viia kasutadaolevad rakendused kooskõlla talitlusnõuetega – õigeaegselt ja mõistlike kuludega rahuldava ning õigeaegse ja kuluefektiivse arendusprotsessi olemasolu tagamisele keskendatud IT-protsessi (rakendustarkvara hankimise ja hooldamise) juhtimine saavutatakse sellega, et

- muundatakse talitlusnõuded kavandamise spetsifikatsioonideks;
- järgitakse arendusstandardeid kõigi muudatuste puhul;
- lahutatakse väljatöötus-, testimis- ja käitustegevused;

ning protsessi mõõtmise näitajad on

- nähtavat seisuaega põhjustavate tootmisprobleemide arv;
- pakutavate funktsioonidega rahul olevate kasutajate protsent."

1.2.2 Juhtimisprotsess TT9 "Hallata konfiguratsiooni" määrab: "Tegevusalast nõuet IT-le – optimeerida IT infrastruktuur, ressursid ja võimed ning pidada IT-varade arvestust – rahuldava ning varade konfiguratsiooni atribuutide ja alusvariantide täpse ja täieliku hoidla rajamisele ja pidamisele ning varade tegeliku konfiguratsiooniga võrdlemisele keskenduv konfiguratsiooni haldamise IT-protsessi juhtimine saavutatakse sellega, et

- rajatakse kõigi konfiguratsioonielementide tsentraalne hoidla;
- piiritletakse konfiguratsioonielemendid ja hooldatakse neid;
- vaadatakse läbi konfiguratsiooniandmete terviklust;

ning protsessi mõõtmise näitajad on

- varade väärast konfiguratsioonist põhjustatud töise kooskõla probleemide arv;
- konfiguratsioonihoidla ja varade tegelike konfiguratsioonide vaheliste tuvastatud lahknevuste arv;
- soetatud, kuid hoidlas arvele võtmata litsentside protsent.

G37 Konfiguratsioonihalduse protsess (jätkub)

1.2.3 Juhtimiseesmärk TT9.1 "Konfiguratsiooni hoidla ja alusvariant" määrab: "Luua abivahend ja tsentraalne hoidla, mis sisaldaks kogu asjassepuutuvat teavet konfiguratsioonielementide kohta. Seirata ja registreerida kõiki varasid ja nende muutusi. Säilitada iga süsteemi ja teenuse konfiguratsioonielementide alusvariant kontrollpunktina, mille juurde saab naasta pärast muudatusi."

1.2.4 Juhtimiseesmärk TT9.2 "Konfiguratsioonielementide identifitseerimine ja hooldus" määrab: "Kehtestada konfiguratsiooniprotseduurid, millega hallata ja logida kõiki muudatusi konfiguratsioonihoidlas. Integreerida need protseduurid muutusehalduse ja probleemihalduse protseduuridega."

1.2.5 Juhtimiseesmärk TT9.3 "Konfiguratsiooni tervikluse läbivaatus" määrab: "Konfiguratsiooniandmeid tuleb perioodiliselt läbi vaadata hetkekonfiguratsiooni ja ajaloolise konfiguratsiooni tervikluse kontrollimiseks ja tõendamiseks. Installeeritud tarkvara tuleb perioodiliselt läbi vaadata tarkvara kasutamise poliitika põhjal, et selgitada välja isiklik või litsentsimata tarkvara või kõik kehtivate litsentsilepetega katmata ülemäärased tarkvara eksemplarid. Kõigist vigadest ja hälvetest tuleb teatada, nende ilmnemisel tuleb tegutseda ning nad tuleb kõrvaldada.

1.3 Toetumine COBITile

1.3.1 Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ning COBITi juhtimiseesmärkide ja nendega seotud juhtimistavade arvestamisel.

1.3.2 Protsessid ja juhtimiseesmärgid, mis tuleb valida ja kohaldada, võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest. Nõuete täitmiseks on valitavad ja kohaldatavad COBITi protsessid, mis on kõige tõenäolisemalt asjakohased, alljärgnevas loetelus jagatud esmasteks ja teisesteks.

Esmajärjekorras:

- PO9 – Hinnata IT-riskid ja hallata neid
- HE6 – Hallata muutusi
- TT9 – Hallata konfiguratsiooni
- SH2 – Seirata ja hinnata sisejuhtimist

Teises järjekorras:

- PO1 – Määratleda strateegiline IT plaan
- PO3 – Määrata tehnoloogiline suund
- PO6 – Teavitada juhtimissihid ja -suund
- TT4 – Tagada pidev teenus

1.3.3 Konfiguratsioonihalduse puhul on kõige asjakohasemad teabekriteeriumid

- esmajärjekorras: toimivus;
- seejärel: tõhusus, käideldavus, usaldatavus.

G37 Konfiguratsioonihalduse protsess (jätkub)

1.3.4 Konfiguratsioonihalduse puhul on kõige asjakohasemad IT halduse keskendumisalad

- esmajärjekorras: väärtuse väljastus;
- teises järjekorras: riskihaldus.

1.4 Suunise eesmärk

1.4.1 Konfiguratsiooni haldamine tähendab mõistliku kinnituse saamist riistvara ja tarkvara konfiguratsioonide tervikluse ning see nõuab täpse ja täieliku konfiguratsioonihoidla rajamist ja hooldamist. See protsess hõlmab algse konfiguratsiooniteabe kogumist, alusvariantide kehtestamist, konfiguratsiooniteabe verifitseerimist ja auditeerimist ning konfiguratsioonihoidla ajakohastamist vastavalt vajadusele. Toimiv konfiguratsioonihaldus soodustab süsteemide käideldavuse suurenemist, minimeerib tootmisprobleeme ja lahendab probleemid kiiremini.

1.4.2 Nüüdisettevõtted on organiseeritud teatava tuumprotsesside kogumina. Peaaegu igal organisatsioonil maailmas tuleb tunda üha tugevamat toimivuse ja tõhususe saavutamise survet (see tähendab kõrgemaid kvaliteedinõudeid toodetele ja teenustele, suuremat tulu, kulude kärpimist, uute toodete väljatöötamist), survet sellise parema, kiirema ja odavama kogu ettevõtet hõlmava süsteemide ja võrgu muutuste ohje protsessi saamiseks, mis annaks ettevõtte omanikele kvaliteetset tarkvara. Mitmesuguste komponentide, näiteks töölauatarkvara, võrkude, vahetarkvara, operatsioonisüsteemi ja andmebaasi süsteemitarkvara muutmisega kaasneb aga oluline risk ja seda tuleks hallata.

1.4.3 See suunis on mõeldud abistama IS audiitorit konfiguratsioonihalduse protsessi läbivaatuse sooritamisel. See dokument on mõeldud eeskätt IS audiitoritele – nii sise- kui ka välisaudiitoritele – kuid seda võivad kasutada ka teised IS ala töötajad, kes vastutavad infosüsteemi käideldavuse, andmete tervikluse ja teabe konfidentsiaalsuse eest.

1.4.4 See suunis kirjeldab konfiguratsioonihalduse järgmisi aspekte:

- protsessi kulg,
- rollid ja kohustused,
- varade jälgimine ja selle vahendid,
- muutuste ohje ja logimine,
- väljastuse haldust hõlmavad teavitusnõuded,
- näitajad aruandluseks.

1.5 Taust ja üldine protsessi kulg

1.5.1 Konfiguratsioonihalduse protsessi siht on

- hallata ja toimivalt ohjata ettevõtte IT-süsteemide, -ressursside ja -võrkude muudatusi, säilitades seejuures süsteemide käideldavuse või suurendades seda;

- suurendada võimalike muudatustest tulenevate riskide toime prognoosimise täpsust ja hallata neid riske;
- luua tsentraalne hoidla kõigile konfiguratsioonielementidele ja ajaloolisele teabele konfiguratsiooni alusvariandi kõigi muudatuste mõju (näiteks teatavat tüüpi muudatuste edu või ebaedu kohta, eelkõige suuremastaabilistes ja keerulistes keskkondades) kohta ja hallata seda;
- teatada kõigi lähiajaks ja kaugemaks tulevikuks plaanitud muudatuste arv ja tüübid, rajades seejuures protsessi, mis teatab kõigile muudatustest mõjutatavatele pooltele muudatuste olekust ja olemasolust.

1.5.2 Toimiv konfiguratsioonihaldus võimaldab juhtkonnal vähendada taganemise riski, mille tekitavad puudulikud ettevalmistused ja/või ühildumatud muudatused, mis mõjutavad süsteemide käideldavust ja andmetöötluse terviklust.

2 AUDITI KAALUTLUSI

2.1 Tüüpilised konfiguratsioonihalduse läbivaatuse objektid

2.1.1 IS audiitor peaks koguma konfiguratsioonihalduse juhtimisprotsessi kohta auditi asitõendeid sõltuvalt organisatsiooni suurusest ja keerukusest. IS audiitor peaks välja selgitama kõrgema juhtkonna ootused konfiguratsioonihalduse alal. Tavaliselt kujutab nõrk konfiguratsioonihaldus endast ohtu süsteemi käideldavusele ja andmete terviklusele. Täpsemalt, ettevõtte süsteemide, ressursside ja võrkude konfiguratsioonimuutuste ning kriitiliste süsteemitõrgete, halva andmetervikluse ja organisatsiooni teabe konfidentsiaalsuse puudumise vahel on tugev korrelatsioon.

2.1.2 IS audiitor peaks õppima tundma konfiguratsioonihalduse poliitikat ja protseduuri, mis visandab teavitusnõuded, sealhulgas dokumenteerimisnõuded ettevõtte süsteemide ja võrkude üksikkomponendi tarkvara ja riistvara muutmisele.

2.1.3 IS audiitoril tuleks saada üldine ettekujutus kõigist ettevõtte süsteemide ja võrkude koostisse kuuluvatest elementidest, sealhulgas kõigist tarkvara (näiteks tööalase rakendustarkvara, vahetarkvara ja andmebaasi süsteemitarkvara) ja riistvara vahelistest seostest ja integratsioonist. Näiteks riistvara tüüpi, mudeli tähist ja sarjanumbrit üheseks identifitseerimiseks.

2.1.4 IS audiitor peaks hankima kogu riistvara- ja tarkvarateabe (mudeli ja sarjanumbri) IT-varade jälgimise süsteemist või sellega võrreldava teabe, mille täielikkus on tõendatud. Kui seda ei ole saadaval, tuleb võib-olla korraldada täielik inventuur.

2.1.5 IS audiitor peaks teadma iga komponendi kohta süsteemis ja ta seoseid kõigi teiste komponentidega.

2.1.6 Tavaliselt tuleb konfiguratsioonihalduse protsessi läbivaatusel

- kontrollida, kas on rajatud kõigi konfiguratsioonielementide tsentraalne hoidla;
- identifitseerida konfiguratsioonielemendid ja säilitada konfiguratsiooniandmed;

G37 Konfiguratsioonihalduse protsess (jätkub)

- teha kindlaks, kas hoidla sisaldab kogu vajalikku teavet komponentide, seoste ja sündmuste kohta;
- teha kindlaks, kas konfiguratsiooniandmed on kooskõlas müüja või teenuseandja kataloogidega;
- teha kindlaks, kas omavahel seotud protsessid on täielikult integreeritud ja kas organisatsioon kasutab ja ajakohastab konfiguratsiooniandmeid automatiseeritult;
- saada mõistlik kinnitus konfiguratsiooniandmete terviklusele;
- kontrollida süsteemi muudatuse formaalse taotluse, sealhulgas muudatuse täieliku dokumentatsiooni olemasolu;
- teha kindlaks, kas muudatuste tuvastuseks ja ettevõtte süsteemide, ressursside ja võrkude riskitasemete järgi liigitamiseks kasutatakse järjekindlalt mingit formaliseeritud meetodit;
- määrata auditi asitõendid taotletava muudatuse riski kaalutlemiste kohta, mida peab vajalikuks konfiguratsioonihalduse komisjon või asjakohane juhtkonna tase. Riski kaalutlemine peaks näitama, kas muudatus piirdub teatud keskkondade või võrkudega, kui suurt töiste kasutajate arvu võib muudatus mõjutada ja kui oluline on ettevõttele infotöötlus;
- kontrollida tegevusalase ja IT juhtkonna formaalset riski kaalutlemise tulemuste (näiteks tulemüüri häälestuse muutmise) kinnitust;
- teha kindlaks, kas on olemas reguleeritav muudatuse väljatöötamine või tarnija ajakohastustoote installeerimine (st süsteemiinseneri "liivakast");
- kontrollida, kas testimisel, mis reservatsioonideta kinnitas konfiguratsiooni muudatused testkeskkonnas, mis kajastab tootmiskeskkonda infrastruktuuris ja töötarkvaras, ei ilmnenud mingit mõju ettevõtte süsteemide, ressursside ja võrkude teistele elementidele;
- kontrollida, kas muudatuste ajakava põhineb koordineerimisel muude muudatustega, nii et võimalik toime ettevõtte süsteemidele, ressurssidele ja võrkudele oleks minimaalne. Selle ajakava koostamine toimub väljastuse halduse alamprotsessi kaudu, mis reguleerib tarkvara käikuandmiste komplekteerimist ning muudatuste sünkroniseerimist, mis minimeerib talitluse mõjutamist;
- teha kindlaks, kas muudatuse üleviimine tootmiskeskkonda toimub reguleeritult (väljaspool tööaega), kusjuures muudatust testitakse täiendavalt tegelikus tootmiskeskkonnas (näiteks hinnatakse andmebaasisüsteemi tarkvara sel teel, et käitatakse olulisi salvestatud protseduure ja päästikuid, hinnates andmeterviklust);
- kontrollida, kas on rajatud kõigi varade, konfiguratsiooniatribuutide ja alusvariantide hoidla. Kontrollida, kas konfiguratsiooni alusvarianti säilitatakse kontrollpunktina, mille juurde saab naasta pärast muudatusi;
- kontrollida, kas alusvariandi kirjeldus esitab iga üksikkomponendi riistvara ja tarkvara kohta olulisi andmeid remondi, hoolduse, garantiimenetluse, ajakohastuse ja tehnilise hindamise tarbeks;

G37 Konfiguratsioonihalduse protsess (jätkub)

- läbi vaadata tegelik varade konfiguratsioon, kontrollides selle vastavust hoidlas olevatele alusvariantidele ja konfiguratsioonihoidla terviklust;
- teha kindlaks, kas on kehtestatud reeglid lubamatu tarkvara avastamiseks ja selle installeerimise vältimiseks ning kas kohustatakse neid järgima;
- teha kindlaks, kas on kasutusel remontide ja ajakohastuste prognoosimise süsteem, mis võimaldab ka ajakavastada versioonitäiendusi ja tehnoloogia uuendusi;
- saada mõistlik kinnitus sellele, et muutuste halduse protsessi ja konfiguratsioonihalduse vahel on seos, nii et konfiguratsiooni läbivaatuse protsessis on muudatuste kõik aspektid arusaadavad.

2.2 Rollid ja kohustused

2.2.1 IS audiitor peaks hankima konfiguratsioonihaldust toetavate rollide ja kohustuste loetelu. Need rollid ja kohustused peaksid olema võetud iga IT-komponendi ja sellega seotud käsitlusala eest vastutava IT-juhtkonna ametijuhenditesse. Kui sellist loetelu ei ole, peaks IS audiitor uurima vastutust konfiguratsioonihalduse eest (st selgitama välja kogu selle protsessi omaniku).

2.2.2 Tuleks hankida teavet ja kontrollida, kas juhtkonnal on piiritletud ressursid, mida on vaja ettevõtte süsteemides, ressurssides ja võrkudes tehtavate muudatuste arvu ja iseloomu mõõtmiseks.

2.2.3 Vastutus selgitatakse välja arvestades esimese ja teise taseme tuge konfiguratsiooni muudatustele.

2.3 Varade jälgimine ja selle vahendid

2.3.1 Varade kaitseks varguse, kuritarvituse või väärkasutuse eest tuleks varasid jälgida ja iga vara seirata.

2.3.2 Tarkvara tuleks märgistada, inventeerida ja asjakohaselt litsentsida. Programmide muudatuste kontrolljälgede loomiseks ning programmide versiooninumbrite, loomise aja teabe ja eelmiste versioonide eksemplaride säilitamiseks tuleks kasutada teegihalduse tarkvara.

2.3.3 IS audiitor peaks hankima kogu lubatava tarkvara loetelu, võimaluse korral sellise, mis on saadud automatiseeritud vahenditega, millega skaneeritakse kõiki riistvaraseadmeid, sealhulgas servereid ja lauaarvuteid. Selline tarkvara väljastab olulised üksikasjad, näiteks

- riistvara tüübi ja mudeli tähise;
- tarkvaraelemendid, sealhulgas liideseprogrammid ja juhtimisvahendid, koostalitlusvõime kontrollimiseks;

G37 Konfiguratsioonihalduse protsess (jätkub)

- ostutarkvara

  - versioon;

  - tarnija toe hetkenõuete dokumentatsioon;

  - kõigi tarnijalt saadud alusvariandis tehtud ja liidestust muu tarkvaraga mõjutada võivate kohanduste dokumentatsioon.

2.3.4 IS audiitor peaks omandama üldise ettekujutuse tarkvara hankimise meetmetest, millega kontrollitakse, kas kogu ostetud tarkvara on IT varade jälgimise süsteemis registreeritud.

2.4 Muudatuste ohje ja logimine

2.4.1 Kasutusel peaksid olema protseduurid, millega kontrollida, kas pärast hankimist kantakse inventari loetellu ainult lubatavad ja identifitseeritavad konfiguratsiooniüksused. Need protseduurid peaksid hõlmama ka konfiguratsiooniüksuste lubatavat kõrvaldamist ning sellele järgnevat müüki või hävitamist.

2.4.2 Kasutusel peaksid olema protseduurid, millega jälgida konfiguratsiooni muudatusi (näiteks: uus element, olekumuutus väljatöötamisel olevast prototüübiks). Logimine ja ohje, sealhulgas muudatuste kirjete läbivaatused, peaksid olema konfiguratsiooni registreerimise süsteemi lahutamatu osa.

2.5 Väljastuse haldust hõlmavad teavitusnõuded

2.5.1 IT kõrgemast juhtkonnast ja tegevusalasest juhtkonnast moodustatud suunamiskomisjon hindab suurt riski tekitavaid konfiguratsiooni muudatusi (näiteks töörakendustes). Muudatuste teostamist puudutavaid otsuseid sisaldavad protokollid tuleks dokumenteerida.

2.5.2 IS audiitor peaks hankima auditi asitõendeid muudatuste ajakava kohta. See ajakava peaks sisaldama väljastuskalendri, millesse on märgitud mitmesuguste muudatuste tootmiskeskkonda üleviimise kuupäevad ja kellaajad. Tavaliselt peaks IS audiitor jälgima muudatuste üleviimise eraldamist, nii et arvutitöö saaks tuvastada olulisi süsteemiprobleeme.

2.5.3 Auditi asitõendid selle kohta, et ettevõtte omanikele on teatatud olulistest konfiguratsiooni muudatustest, nii et nad oleksid valmis avastama ebaharilikke süsteemisündmusi.

2.6 Näitajad aruandluseks

2.6.1 Kõik näitajate väärtused, sealhulgas mõõtepaneelidel, saadakse ettevõtte süsteemide, ressursside ja võrkude muudatuste arvu ja iseloomu mõõtmise tulemusena. Mõned tüüpilised mõõdetavad näitajad:

- keskmine ajavahemik (hilistumine) mingi hälbe avastamisest selle kõrvaldamiseni;

- puuduliku või puuduva konfiguratsiooniteabega seotud hälvete arv;
- sooritusvõime, turvalisuse ja käideldavuse teenusetasemetele vastavate konfiguratsiooniüksuste arv;
- konfiguratsioonihoidla ja varade tegelike konfiguratsioonide vahel ilmnenud lahknevuste arv;
- soetatud, kuid hoidlas arvestamata jäänud litsentside arv;
- volitamata litsentside protsent kasutuselolevatest soetatud litsentsidest;
- varade ebasobivast konfiguratsioonist tingitud tegevusalase vastavuse probleemide protsent.

2.6.2 Formaalselt dokumenteeritakse ja levitatakse IT juhtkonna hulgas sooritusnäitajaid, sealhulgas teenusetaseme statistikat reaktsiooniaja, süsteemi tööaja (käideldavuse), andmetervikluse kvaliteedi jms kohta. Nende näitajatega tuleks mõõta töötajate või allettevõtjate (IT-teenuste väljasttellimise puhul) sooritust.

2.6.3 Muudatuste puhul tuleks teha kindlaks, kas juhtkond mõõdab teostusaega ning kas sellest sõltub alljärgnevat arvestades häirimiseta muutmise õnnestumine või nurjumine.

- Kui teostusaeg on tähtis, tuleb häirimise vähendamiseks välja selgitada tundlikud muudatuste tüübid ja mahud.
- Määrata parem meetod muudatuste identifitseerimiseks ja riskitasemete järgi liigitamiseks.
- Kontrollida, kas iga kirje on tehniliselt ja halduslikult jälitatav.
- Kehtestada verifitseerimisprotsess kirjete järjekindlaks läbivaatuseks tehniliste eeliste ja talitlusvalmiduse seisukohalt, kusjuures tuleb võimaldada paindlikkust tegevusalaste vajaduste põhjal.

3 JÕUSTUMISKUUPÄEV

3.1 See suunis kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. novembril 2007 või pärast seda.

G38 Pääsu reguleerimise meetmed

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S1 "Audititalituse põhikiri" määrab: "Infosüsteemide auditi talituse või infosüsteemide auditi ülesande täitja eesmärk, kohustused, õigused ja vastutus peaksid olema auditi põhikirjas või töövõtukirjas selgelt dokumenteeritud."

1.1.2 Standard S3 "Kutse-eetika ja standardid" määrab: "IS audiitor peaks järgima ISACA kutse-eetika koodeksit."

1.2 Seos suunistega

1.2.1 G13 "Riski kaalutlemise kasutamine auditi plaanimisel" määrab: "Valitud riski kaalutlemise meetodeid peaks IS audiitor kasutama üldise auditiplaani koostamisel ja konkreetsete auditite plaanimisel. Riski kaalutlemisele kombineeritult muude auditi meetoditega tuleks mõelda näiteks selliste plaanimisotsuste tegemisel:

- auditiprotseduuride iseloom, ulatus ja ajastus;
- auditeerimisele kuuluvad alad või talitlusfunktsioonid;
- auditile eraldatav aeg ja ressursid.

1.3 Seos COBITiga

1.3.1 Juhtimisprotsess SH2 "Seirata ja hinnata sisejuhtimist" määrab: "Sisejuhtimise seire ja hindamise IT-protsessi juhtimine, mis rahuldab ärinõuet IT-le kaitsta IT eesmärkide saavutamist ja järgida IT-ga seotud õigusakte, keskendudes selleks IT-ga seotud tegevuste sisejuhtimise protsesside seirele ja piiritledes täiustusmeetmed, saavutatakse sellega, et

- määratletakse IT-protsessi raamstruktuuris olev sisemeetmete süsteem;
- seiratakse IT-le rakendatud sisemeetmete toimivust ja teatatakse tulemustest;
- teatatakse juhtkonnale tegutsemiseks ootused juhtimise kohta.

SH2 mõõdud on

- suuremate sisejuhtimise tõrgete arv,
- juhtimise täiustamise ürituste arv,
- juhtimise enesehindamiste arv ja katvus.

1.3.2 SH3 "Tagada vastavus välisnõuetele", mis rahuldab ärinõuet IT-le tagada vastavus seadustele, eeskirjadele ja lepingunõuetele, keskendudes selleks kõigi kohaldatavate seaduste, eeskirjade ja lepingute ning IT vastavustasemete väljaselgitamisele ja IT-protsesside optimeerimisele lahknevusriski vähendamiseks, saavutatakse sellega, et

- selgitatakse välja IT-d puudutavad seaduste, eeskirjade ja lepingute nõuded,

- hinnatakse vastavusnõuete mõju;
- seiratakse vastavust neile nõuetele ja teatatakse tulemustest.

SH3 mõõdud on

- IT lahknevuse hind, sealhulgas hüvitused ja trahvid,
- keskmine hilistus välisnõuete probleemide väljaselgitamise ja nende lahendamise vahel,
- vastavuse läbivaatuste sagedus.

1.3.3 SH4 "Tagada IT haldus", mis rahuldab ärinõuet IT-le integreerida IT haldus organisatsiooni halduse eesmärkidega ning järgida seadusi, eeskirju ja lepinguid, keskendudes selleks aruannete koostamisele juhatusele IT strateegia, tulemuste ja riskide kohta ning reageerides haldusnõuetele kooskõlas juhatuse suunistega, saavutatakse sellega, et

- rajatakse IT halduse raamstruktuur, mis on integreeritud üleorganisatsioonilise haldusega;
- saadakse sõltumatu kinnitus IT halduse seisundi kohta.

SH4 mõõdud on

- direktsiooni aruannete sagedus huvipooltele IT (sh küpsuse) kohta;
- direktsioonile esitatavate aruannete sagedus IT (sh küpsuse) kohta;
- IT vastavuse sõltumatute läbivaatuste sagedus.

1.4 Toetumine COBITile

1.4.1 Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ning arvestades COBITi juhtimiseesmärke ja nendega seotud haldustavasid. IS audiitorile õiguste, kohustuste ja vastutuse kohta esitatavate nõuete täitmiseks on alljärgnevas need COBITi protsessid, mille asjakohasus, valimine ja rakendamine on kõige tõenäolisem, jagatud esmasteks ja teisejärgulisteks. Protsess ja juhtimiseesmärgid, mis tuleb valida, võivad varieeruda sõltuvalt ülesande lähtetingimustest.

1.4.2 Käesoleva suunisega käsitletava ala läbivaatusel tuleks esmasteks lugeda järgmised spetsiifilised COBITi eesmärgid või protsessid:

- PO1 – Määratleda strateegiline IT plaan;
- PO2 – Määratleda infoarhitektuur;
- PO9 – Hinnata IT riskid ja hallata neid;
- TT5 – Tagada süsteemide turvalisus;
- TT7 – Koolitada kasutajaid;
- TT9 – Hallata konfiguratsiooni.

G38 Pääsu reguleerimise meetmed (jätkub)

1.4.3 Käesoleva suunisega käsitletava ala läbivaatusel tuleks teisejärgulisteks lugeda järgmised spetsiifilised COBITi eesmärgid või protsessid:

- PO6 – Teavitada juhtimissihid ja suund;
- PO7 – Hallata IT inimressursse;
- HE1 – Tuvastada automatiseeritud lahendused;
- HE2 – Hankida rakendustarkvara ja hooldada seda;
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda;
- HE6 – Hallata muutusi;
- TT1 – Määratleda teenusetasemed ja hallata neid;
- TT2 – Hallata kolmandate poolte teenuseid;
- TT10 – Hallata probleeme;
- TT12 – Hallata füüsilist keskkonda;
- SH1 – Seirata ja hinnata IT töötulemusi;
- SH3 – Tagada vastavus välisnõuetele.

1.4.4 Kohustuste, õiguste ja vastutuse seisukohalt kõige asjakohasemad teabekriteeriumid on

- esmajärjekorras: toimivus, tõhusus ja konfidentsiaalsus;
- teises järjekorras: käideldavus, terviklus ja usaldatavus.

1.5 Suunise eesmärk

1.5.1 Tegelikus kokkuühendatud maailmas peaksid organisatsioonid kaitsma oma varasid volitamata kasutamise eest ning kaitsma mitte ainult oma investeeringuid, vaid kaitsma ka infovarasid ressursside sihilikust või ettekavatsematust väärkasutusest tingitud riskide eest. Tegelikud tehnoloogia rakendused (näiteks platvormid, rakendused, utiliidid, operatsioonisüsteemid, andmebaasid, meiliprogrammid, turbe ja auditeerimise instrumendid, Internet, faks) on väga mitmekesised ja keerukad ning kõiki neid tuleb kaitsta volitamata kasutamise eest. Kaitsta tuleb ka füüsilised varad, näiteks hooned, seadmed, sidesüsteemid, paljundid, kaamerad, dokumendikapid, üldine trükitud teave ja kliendidokumentatsioon. Sellise mitmekesisuse tõttu on eluliselt tähtis kasutada üht standardset protsessi juurdepääsu reguleerimiseks. Sellest standardist saab etalon, mis on kohandatud hoolitsema organisatsiooni erivajaduste eest.

1.5.2 See suunis annab juhiseid IS auditeerimise standardite S1 ja S3 rakendamise kohta. IS audiitor peaks seda suunist arvestama otsustamisel, kuidas jõuda ülalnimetatud standardite rakendamiseni, kasutama selle rakendamisel kutsealast otsustusvõimet ning olema valmis põhjendama iga lahknevust.

G38 Pääsu reguleerimise meetmed (jätkub)

1.6 Suunise rakendamine

1.6.1 Selle suunise rakendamisel peaks IS audiitor arvestama ta juhiseid seoses muude asjassepuutuvate ISACA standardite ja suunistega.

1.7 Üldised pääsuklassid

1.7.1 Minimaalne pääs: kasutaja juurdepääs ainult spetsiifilistele vajalikele ressurssidele.

1.7.2 Teadmistarbeline pääs: kasutaja juurdepääs ressurssidele, mida ta vajab töö tegemiseks organisatsioonile, mitte isiklikes huvides.

1.7.3 Omanik: vara eest vastutav kasutaja.

2 ÜLDISED MÄÄRATLUSED

2.1 Turvapoliitika

2.1.1 Turvapoliitika on üldtaseme dokument, mis kirjeldab juhtkonna ja organisatsiooni kohustusi ning määratleb turvastrateegia, mis vastab tegevusalastele eesmärkidele. Täielikuks rakendamiseks tuleks sõnastada standardid ja protseduurid. Standardid määratlevad, **mida** tuleks teha poliitika järgimiseks ja on mõeldud kõigile lugejaskondadele. Protseduurid kirjeldavad, **kuidas** seda tuleks teha ja on mõeldud neile, kellel tuleb poliitikat ellu viia (näiteks kasutajate, tehnoloogia, tarnijate alal). Ülalloetletu võib korraldada eraldi dokumentideks, kuid neid võib ka ühendada **pääsu reguleerimise poliitikaks**.

2.1.2 On palju teabeallikaid, mida arvestada turvapoliitika koostamisel. Iga organisatsioon peaks seda teavet hindama oma tegevuse, kaitsevajaduse ja kultuuri seisukohalt ning rakendama seda, mis kõige paremini vastab ta eesmärkidele. Poliitika peaksid koostama põhitegevuse ja turbe spetsialistid ning enne poliitika teatavaks tegemist kõigile töötajaile ja neilt selle kohta allkirjade võtmist peaks poliitikale andma kinnituse tippjuhtkond või juhatus.

2.2 Pääsureeglite määratlemise kriteeriumid

2.2.1 Üldiselt peaksid kriteeriumid põhinema teadmistarbe põhimõttel. Iga organisatsioon peab määratlema igale töötajate, tarnijate, klientide, reguleerijate ja audiitorite rühmale sobiva (näiteks rollipõhise) pääsutaseme. Tuleks teha täielik infovarade inventuur, arvestades seejuures teabe tähtsust, haavatavust, olemasolevaid turvameetmeid IT-keskkonnas, teabe töötlemise seadmeid ning teabe haldajate oskusi ja eriteadmisi (intellektuaalset omandit). Kaitset vajavate füüsiliste varade või ressursside hulka kuuluvad

- hooned koos nende elektritoite, turbe ja muu infrastruktuuri komponentidega (näiteks katkematu toite allikate, generaatorite, kaameratega);

G38 Pääsu reguleerimise meetmed (jätkub)

- andmetöötluskeskused;
- sidesüsteemide ruumid (kus on kommutaatorid, jaoturid, marsruuterid, telefonijaamad, kaablid);
- teegid (lindid, kassetid, arhiivikettad);
- soomuskambrid, tulekindlad seifid;
- turvalaekad ja võtmelaekad;
- faksid;
- paljundid;
- teleks;
- kliendidokumentatsioon;
- abidokumentatsioon (regulatiivne).

2.2.2 Organisatsioon peaks elutähtsate kohustuste lahususe kontrollimiseks kaaluma pääsurollide maatriksi loomist ja selle perioodilist läbivaatust.

2.2.3 Kaitset vajavate loogiliste varade või ressursside hulka kuuluvad

- serverid (st veebiserverid, rakendused) ja nende operatsioonisüsteemid;
- andmebaasisüsteemid või failisüsteemid;
- rakendused;
- utiliidid ja instrumendid;
- magnetkaardid, võtmed, tunnistused ja kiipkaardid;
- serverid, tööjaamad ja telefonijaam;
- andmed üldse;
- e-post (organisatsiooni kontod);
- tulemüür ja/või sissetungi tuvastuse süsteem (IDS);
- aruanded;
- revisjonilogid;
- võrk (turvaperimeeter).

2.3 Omanikud ja nende kohustused

2.3.1 Igale infovarale (ja IT-ga seotud füüsilisele varale) tuleks formaalselt määratleda omanik koos talle määratud kohustustega. Kohustused peaksid hõlmama seda, et teabe omaniku kohus on tagada pääsu reguleerimise põhimõtete ja reeglite olemasolu, rakendatus ja järgimine organisatsioonis.

G38 Pääsu reguleerimise meetmed (jätkub)

2.4 Varade liigitus

2.4.1 Varade liigitus peaks põhinema hallatava teabe tüübil (näiteks: kitsendustega, konfidentsiaalne, sisemine, avalik).

2.5 Administreerimine

2.5.1 Pääsu reguleerimise poliitika peaks selgelt määratlema kohustused, rollid ja protseduurid muudatuste tegemiseks töötaja staatuses, näiteks ametikohtade ja tööülesannete muutmiseks ning üleviimiseks sama osakonna või infoturbeala (ISA) piires. Väga tähtis on kehtestada protseduur, millega hallata muudatusi kasutaja staatuses ning teha need muudatused teatavaks teabe omanikele, kasutajatele, eeliskasutajatele, järelevalvajaile või muudele isikutele või allüksustele, kelle kohus on õiguste määratlemine, andmine, äravõtmine või muutmine. Üldine vastutus turbe administreerimise eest peaks olema turvaadministraatoril. "Õigused" tähendavad siin kasutajaile tagatavaid pääsuõigusi.

2.6 Kasutajameetmed

2.6.1 Kasutajate tegevuste reguleerimiseks ja seireks tuleks määratleda vastav meetmestik, näiteks kasutajate blokeerimiseks pärast teatavat arvu järjestikku nurjunud sisselogimisi ja jõudeolekus kasutajate blokeerimiseks või kõrvaldamiseks pärast mingit ettemääratud jõudeperioodi. Edukalt sisseloginud kasutaja kohta tuleks registreerida nurjunud katsete arv ning eduka sisselogimise kuupäev ja kellaaeg.

2.7 Õiguste läbivaatus

2.7.1 Vähemalt kord poolaastas tuleks korraldada õiguste läbivaatusi, millega kontrollida, kas omanikud või järelevalvajad kinnitavad kasutajate õigusi ja tehtud muudatusi. Õiguste läbivaatuse sooritamist nõudva protseduuri sobivust tuleks hinnata vähemalt kord aastas, et kontrollida, kas keskkonnas (st rakendustes, välisvõrku pääsus) on mingeid muutusi, mille tõttu võiks tekkida vajadus kaaluda õiguste sagedamat läbivaatamist.

2.8 Volitatud kasutamine ja karistused

2.8.1 Poliitika ja selle tugidokumendid (st standardid, suunised) peaksid muude riskiatribuutide käsitlemisel määrama, et organisatsiooni ressursse tohib kasutada ainult töiseks otstarbeks ja neid ei tohi kasutada isiklikes huvides. Ettevõtte ressursside väärkasutuse või ebasobiva kasutamise eest tuleks rakendada karistusi või sanktsioone.

2.8.2 Poliitika peaks hõlmama reguleerivat raamistust (üleorganisatsioonilist ja kohalikku), sealhulgas privaatsusseadusi, andmekaitset või pangasaladust. Ta peaks ka teatama, millised toimingud on keelatud, näiteks osalemine kettkirjades, tarkvara allalaadimine Internetist, isikliku CD-del või diskettidel oleva tarkvara kasutamine või organisatsioonile kuuluva teabe kasutamine isiklikes huvides.

G38 Pääsu reguleerimise meetmed (jätkub)

2.9 Välised töötajad

2.9.1 Poliitika peaks ütlema, millised funktsioonid või tehingud (näiteks turbetehingud, volitamine) ei ole kättesaadavad ajutistele konsultantidele või kolmanda poole personalile. Juurdepääs neile funktsioonidele ja tehingutele on võimalik võrgumeetmete kaudu, kuid nad ei ole kättesaadavad organisatsiooni meili, sissehelistusühenduse jms kaudu.

2.10 Vastutus ja parooli jagamine

2.10.1 Poliitika peaks selgelt teatama, et iga töötaja vastutab tema parooliga tehtud toimingute eest ka siis, kui tõestatakse, et toimingu sooritas tema parooliga teine isik. Paroolidel peaks olema kehtivustähtaeg ja süsteemid peaksid automaatselt sundima paroole vahetama. Iga organisatsioon määratleb kõigi eelnimetatud elementide põhjal pääsunõuded vastavalt töötaja või kliendi tööalastele hetkevajadustele ja juriidilisele keskkonnale.

2.11 Pöörduse tüüp

2.11.1 Pöördumise lähtekoha järgi võib pöördust liigitada kohalikuks ja kaugpöörduseks. Kohaliku pöörduse lähtekoht on selle organisatsiooni sees, kus ressursid füüsiliselt asuvad. Kaugpöörduse lähtekoht on muudes asukohtades, näiteks kodus, ja enamasti kasutatakse seda muutuseohje protseduurideks hädaolukorras või administraatori plaanitud operatsioonideks. Viimasel juhul tuleks mõelda spetsiaalsetele turvameetmetele, nagu seda on konfigureerimise ja viirusetõrje tarkvara, ühenduse turve (virtuaalsed privaatvõrgud (VPN), krüpteerimine, SSL) ja igapäevane koduarvutitel sooritatavate kaugtegevuste reguleerimine.

2.11.2 Traadita või mobiilseadmete kasutamine tuleks minimeerida (mitte kasutada elutähtsate protsesside ja elutähtsa teabe puhul) ning rangelt reguleerida. Pöörduse liigitamisel tehniliseks ja mittetehniliseks ning struktureerituks ja struktuurituks tuleb arvestada pöörduse sooritamise keerukust ja vajalikke oskusi. See on väga tähtis riskianalüüsi sooritamise ning toimumise tõenäosuse määramise jaoks.

2.12 Pääsuvahendid

2.12.1 Juurdepääsu infovaradele tuleks mõõta identifitseerimise, autentimise, volitamise või salgamistõrje põhjal.

2.12.2 Kasutaja tuleks ressursile identifitseerida, tavaliselt kasutaja identifikaatoriga (ID, vähemalt kaheksakohaline numbri- ja märgijada), ID-kaardiga või füüsilise (biomeetrilise) identifikaatoriga, näiteks isiku hääle, sõrmejälje, silma vikerkesta või silma võrkkestaga.

2.12.3 Kasutaja tuleks autentida sel teel, et ta esitab ressursile salajase objekti, mis tõendab, kes ta on. Mida kasutada autentimiseks, sõltub liigitusest ja riski hinnangust; autentimisvahenditeks võivad olla staatilised paroolid, dünaamilised ehk ühekordsed

G38 Pääsu reguleerimise meetmed (jätkub)

paroolid (pääsmed), biomeetrikud, isiku identifitseerimise numbrid (PIN-koodid), äripartneri identifitseerimise numbrid (TPIN-koodid). Isiku autentimiseks kasutatakse "midagi, mida ta teab", "midagi, mis tal on" või "midagi, mis ta on". Mitme vahendi kombineerimisel on turve tugevam; näiteks kasutatakse pangaautomaadis kahe vahendiga autentimist: millegagi, mida isik teab (PIN-kood) ja millegagi, mis tal on (kaart). Pääsu reguleerimise poliitika peaks sisaldama näiteks selliseid tabeleid, nagu on alljärgnev.

Teabe liigitus, riski hinnang, rakenduse otstarve ja pöörduse tüüp	**Meetod**			
	PIN/TPIN	**Staatilised paroolid**	**Ühekordsed paroolid**	**Biomeetria**
Avalik teave, väike risk, mittetehingulised rakendused, sisepöördus	1	2	2	2
Konfidentsiaalne teave, keskmine risk, tehingulised rakendused, sisepöördus	0	0	2	2
Kitsendustega teave, suur risk, tehingulised rakendused, kaugpöördus (veeb)	0	0	1	2

Tähistus: 0 - pole piisav, 1 - piisav, 2 - soovitav.

2.12.4 Õnnestunud identifitseerimise ja autentimise korral annab süsteem loa juurdepääsuks kõnealusele ressursile. Kasutatav meetod sõltub ressursi tüübist; näiteid:

- hooned, ruumid, soomuskambrid, andmetöötluskeskused – kasutaja pääsukaardid, PIN-koodid, biomeetria;
- kliendidokumendid, kapid, faksid – kasutaja võtmed, kaardid, järelevalvaja memod;
- tulemüürid ja proksid on seadmevarad, mis võimaldavad juurdepääsu teistele ressurssidele, ning kuna nad on väga tähtsad, tuleks neile anda eriline kaitse. Neil peab olema nii füüsiline kui ka loogiline kaitse kasutamisele ainult administraatori rollis, konfiguratsiooni muutmisele ning alarmide ja logide kasutamisele. Kõigil juhtudel peab iga ettevõte analüüsima oma vajadusi sõltuvalt kasutatavatest teenustest (näiteks veebiteenused, e-post, FTP-d) ning järgima standardite ja parimate tavade soovitusi (näiteks sulgema pordi 80). Selle eesmärgi saavutamiseks on oluline, et iga ettevõte mõtleks sellisele nõrkuste ja ohtude halduse protseduurile, mis sisaldab ühe või mitme turvabülletääni (mida annavad välja näiteks CERT, SANS, Microsoft, NIST);
- sissetungi tuvastuse süsteemid (IDS), aktiivkaitse süsteemid (ADS) ja sissetungi tõrje süsteemid (IPS) on riistvara ja tarkvara, mis avastab ja analüüsib kahtlast liiklust; nad tuleb konfigureerida genereerima alarme ja logisid, mis tuleb viivitamatult läbi vaadata. Tähtis on võtta kasutusele protsess saadud logide ja alarmide läbivaatuseks; nende analüüs näitab muudatusi konfiguratsioonis, sõltuvalt ohtude riskist;

- rakenduste, operatsioonisüsteemi ja andmebaasihalduse süsteemi (DBMS) kasutajaprofiilid, mis on määratletud rakenduse või DBMS-i tasemel. Igale kasutajale kinnistatakse mingid kasutusõigused ja need paigutatakse pääsuloenditesse (ACL);
- lõppkasutajat, kes töötab Exceli arvutustabelitega, Accessi tabelitega või Foxbase'i või Dbase'i failidega, kui need on olemas), tuleks kaitsta arvutustabelite paroolidega, kasutajaõigustega, lahtriparoolidega jms. Neid vahendeid ei ole soovitatav kasutada elutähtsate protsesside puhul, sest nende pakutavad turvameetmed (näiteks paroolkaitse) võivad olla nõrgemad neist, mis on ehitatud rakendustesse või andmebaasihalduse süsteemi.

2.12.5 Salgamise vääramine on mõeldud tagama seda, et tehingu sooritanu ei saa tehingut eitada. Ta teostatakse digitaalallkirjade ja logide abil.

2.13 Riski kaalutlemine

2.13.1 Pääsuriski kaalutlemisi tuleks sooritada pidevalt, vastavalt ohtude iseloomule ja ohustsenaariumi muutustele.

2.13.2 Halvad pääsu reguleerimise tavad võivad viia konfidentsiaalse teabe paljastamiseni (konfidentsiaalsuse rikkumine), andmete volitamata muutmiseni (tervikluse rikkumine) või tegevuse pidevuse katkemiseni (käideldavuse rikkumine). Sobivate pääsu reguleerimise meetmete puudumise tagajärgi tuleks arvestada vara väärtuse põhjal organisatsioonile, nii kvalitatiivsest kui ka kvantitatiivsest vaatepunktist; näiteid: maine langus, kliendi mulje, suutmatus täita kohustusi, järeleandmised (lepingutes, teenusetasemelepetes), regulatiivne toime (trahvid ja sanktsioonid), rahaline toime, konkurentsivõime langus ja tulude kadu. Selle riski minimeerimiseks tuleks rakendada (vastavalt poliitikale) preventiivseid meetmeid ja vähendada risk tasemeni, mis on ettevõttele vastuvõetav (jääkrisk). Protsessi turbeks on vajalikud ka avastamismeetmed.

2.13.3 Mingilt süsteemilt nõutava usaldusastme määravad infovarade väärtus ja neid varasid ähvardav risk.

2.14 Riski seire ja mõõdud

2.14.1 Metoodikates, näiteks juhtimisriski enesehindamise metoodikas, tuleks määratleda pääsuriski näitajad. Näiteid:

- väliste (nurjunud või õnnestunud) sissetungikatsete arv;
- sisemiste volitamata katsete arv;
- volitamatust pääsust tingitud turvaintsidentide arv;
- lahknevustega õiguste läbivaatuste arv;
- pääsutaotluste ebaadekvaatsete aktsepteerimiste arv.

G38 Pääsu reguleerimise meetmed (jätkub)

2.15 Spetsiifilised pääsu ohud

2.15.1 Organisatsioonid peaksid sõltuvalt oma toodetest, teenustest ja rakendustest analüüsima enda avatust inimestega manipuleerimisele, teabe väljapetmisele, identiteedivargusele, teenusetõkestusrünnetele, pettesaitidele veebis ja skriptrünnetele. Potentsiaalse ohtudele avatuse põhjal peaksid nad mõtlema veebirakenduste ja infrastruktuuri turbe erimeetmetele (näiteks veebistandardite poliitikale, eetilisele häkkimisele).

2.15.2 Organisatsioon peaks olema valmis asjakohaselt reageerima pääsurikkele, sealhulgas volitamata sissetungile.

2.16 Vältimismeetmed

2.16.1 Vältimismeetmete hulka kuuluvad alljärgnevad.

- Juurdepääs süsteemile tuleks autentida tugeva parooli abil (reeglid parooli pikkuse ja keerukuse kohta, vahetamise sagedus, parooli jagamine jne).
- Enne juurdepääsu andmist ettevõtte teaberessurssidele peaks selleks olema formaalne luba ettevõtte omanikult.
- Regulatiivseid nõudeid (üleorganisatsioonilisi ja kohalikke) ning poliitikale vastavaid pääsu reguleerimise meetodeid arvestav pääsu reguleerimise poliitika tuleks teatavaks teha kõigile töötajaile ja võtta neilt selle kohta allkiri.
- Tuleks alla kirjutada lepingud personaliga ressursside (inimressursside) õige kasutamise kohta.
- Tuleks kehtestada kava personali koolitamiseks, teavitamiseks ja teadvustamiseks õigest juurdepääsu kohta ning sanktsioonid lahknevuste puhuks.
- Tuleks rakendada omanike ja järelevalvajate kinnitatud protseduurid juurdepääsu määratlemiseks, kinnitamiseks, töötluseks, tühistamiseks, välistamiseks, muutmiseks, teatavaks tegemiseks, logimiseks ja auditeerimiseks.
- Tuleks rakendada administreerimisprotseduure, sealhulgas administreerimisfunktsiooni igapäevase juhtimise meetmeid.
- Kõik tarnija seatud kasutajaidentifikaatorid, mis ei ole tööks vajalikud, tuleks kõrvaldada.
- Selliste tarnija seatud kasutajaidentifikaatorite puhul, mis on tööks vajalikud, tuleks nõuda algse vaikeparooli vahetamist.
- Tuleks rakendada pääsu reguleerimise instrumente, näiteks auditeerimisvahendeid, tulemüüre ja identifikaatoreid.
- Tuleks kehtestada ressursside kasutamise poliitika, mis sisaldab töötajaile kohaldatavaid sanktsioone ressursside (e-post, Internet) väära kasutamise eest.
- Nõuded kolmandate poolte juurdepääsu kohta (teenusetasemelepped või lepingud).

G38 Pääsu reguleerimise meetmed (jätkub)

- Märgistusprotseduurid, mis sõltuvad riskikaalutlustest.
- Kitsendused ajutiste töötajate juurdepääsule (turvafunktsioonid, tehingute volitamine).
- Võimaluse korral vaikepääsu ja vaikekasutajate kõrvaldamine kõigil platvormidel.
- Kõigi tootmiskontode kitsendamine, vältides kasutajate sisselogimist.
- Krüpteerimine lisaks pääsu reguleerimisele nõrgendab volitamata juurdepääsu toimet.
- Protseduurid, millega määratletakse juurdepääs füüsilistele ressurssidele (näiteks arhiivikappidele, faksidele, soomuskambritele, dokumentidele) ning nende nõuded säilitamise ja kaitse kohta.
- Kohustuste lahususe rakendamine: juurdepääs elutähtsatele andmetele jagatakse kahe või mitme isiku vahel, nii et saavutatakse teatav vastastikuse kontrolli tase.
- PIN-kood, TPIN, turvaline Interneti-parool (HPIN), pääsmikud, biomeetria, kasutajaprofiilid, privileegid, seansi kontrollaeg, trosslukk, viirusetõrje, nuhkvara tõrje.

2.17 Avastusmeetmed

2.17.1 Avastusmeetmete hulka kuuluvad alljärgnevad.

- Õiguste läbivaatamise protseduurid, mis hõlmavad lahknevusolukordade käsitluse laiendamist ning tarnijate, klientide, reguleerijate ja audiitorite logimist ja läbivaatust.
- Privileeg- või ülemkasutaja sisselogimiskonto kaudu sooritatavaid toiminguid peaks arvutiturbe kõrgem juhtkond detailselt seirama ja läbi vaatama.
- Ebaadekvaatse juurdepääsu, ressursside kuritarvituse, kahtlaste toimingute ja häkkimise halduseks peaks olema turvaintsidentide protseduur, mis sisaldaks rolle ja kohustusi ning käsitluse laiendamise protseduure.
- Tuleks korraldada õiguste, eeliskasutajate, tegevkasutajate, vaikekasutajate, erigruppide ja -rollide, tulemüüri ja IDSi konfiguratsioonide, alarmide ja logide auditeid ja kvaliteedi tagamise läbivaatusi.
- Siseauditite läbivaatuste täiendamiseks tuleks rakendada enesehindamise metoodikat. Näiteks integreeritakse vastav meetmestik äriprotsessidega ning seda käivitatakse igal alal riskile vastava sagedusega.
- Igal aastal tuleks sooritada hindamine läbistustestiga, mis vastavalt vajadusele hõlmab võrke, inimesi, ressursse ja äriprotsesse.
- Lubamatuid toiminguid sisaldavad tegevused tuleks logida ja läbi vaadata.

G38 Pääsu reguleerimise meetmed (jätkub)

2.18 Korvamismeetmed

2.18.1 Korvamismeetmetele tuleks mõelda siis, kui avastus- või vältimismeetmetest ei piisa.

2.18.2 Kõigile asjakohastele näitajatele tuleks määratleda päästikväärtus, mis võimaldaks turbehalduril analüüsida probleemide põhjusi ja määratleda probleemide leevendamiseks või lahendamiseks haldusmeetmete (näiteks koolituse tugevdamise ja turbevahendite ostmise) plaan.

2.19 Pääsu administreerimise protseduur

2.19.1 See ülesanne võib organisatsioonides varieeruda sõltuvalt kohalikest protseduuridest, platvormidest, utiliitidest ja pääsu administreerimise vahenditest, kuid peaks alati sisaldama alljärgnevat.

- Kõigiks toiminguteks (näiteks lisamisteks, kustutusteks, lähtestusteks ja profiilide muutmiseks) tuleks nõuda formaalselt dokumenteeritud pääsutaotlust koos adekvaatsete põhjendustega ja omaniku kinnitustega.
- Kui administreerimisprotsess on käsiprotsess (vormi või meiliga), peaks kasutajalt taotluse saanud administraator kontrollima, kas taotlusel olevad kinnitused on korras. Mõnedel juhtudel on see protsess automatiseeritud mingi rakendusega, mis sisaldab iga ressursi või ala omaniku või järelevalvaja andmeid ja sooritab kinnituste saamiseks ühe automaatse töövoo.
- Ajavahemik iga kasutajate administreerimise operatsiooni töötluseks peaks olema määratletud ja ettevõttega kokku lepitud (näiteks teenusetasemeleppes, tööülesandes). Näiteks tuleks kasutaja lähtestusele elutähtsates rakendustes tuleks reageerida vastavalt teenusetasemeleppele või sobivalt määratletud ajavahemiku piires.
- Protsess peaks selgelt määratlema selle, kuidas väljastatakse kasutajaile paroolid lisalähtestusteks. Mõnedel juhtudel on see automatiseeritud mingi rakendusega ja administraator ei saa teada kasutajate paroole. Samuti on soovitav, et (näiteks kasutajatehingute lisamise või lähtestuse käigus) genereeritud paroole peaks teadma ainult konto omanik ja paroole tuleks salvestada krüpteeritult, sest neid tuleks lugeda kitsendatud kasutusega teabeks.
- Protsess PIN- ja TPIN-koodide väljastuseks töötajaile või klientidele peaks kasutama teistsugust väljastuskanalit kui pääsuese (kaart, pääsmik) ja need peaksid olema passiivses olekus, kuni nad jõuavad omanikuni, kes saab neid aktiveerida.
- Peaks olema mingi mehhanism, mis tagab parooli, PIN-koodi või TPIN-koodi hävitamise juhul, kui parool või kood ei jõua mingi ajavahemiku jooksul kasutajani.

G38 Pääsu reguleerimise meetmed (jätkub)

2.20 Infoturbe administreerimise ohje meetmed

2.20.1 Meetmed hõlmavad alljärgnevat.

- Kõik infoturbe administreerimise toimingud tuleks jäädvustada revisjonilogides.
- Kõik kasutajate administreerimise ülesanded tuleks lahutada kõigist muudest tegevustest (näiteks süsteemide administreerimisest, äritehingutest ja arendustegevusest), muidu võib puudulik kohustuste lahusus viia huvide vastuoludeni.
- Kontrollimaks, kas töödeldakse ainult vajalikke toiminguid, peaks mingi sõltumatu pool kontrollima kõiki infoturbe administreerimise toiminguid 24 tunni kestel või rakendama tegija ja kontrollijaga kaksikkontrolli.
- Eeliskasutajaid (administraatoreid, andmebaasihaldureid) tuleks seirata ja neile tuleks põhjendamise, dokumenteerimise ja kinnitamise osas rakendada rangemat ohjeprotsessi.

2.21 Kasutajate toimingute ohje meetmed

2.21.1 Kasutajate toimingute ohje meetmed hõlmavad alljärgnevat.

- Korduvad nurjunud sisselogimiskatsed tuleks tuvastada ja neid tuleks uurida.
- Igat (kolme või enama järjestikku nurjunud katse järel) blokeeritud või peatatud kasutaja identifikaatorit tuleks uurida, kontrollides, kas kasutaja on selle identifikaatori õige omanik, mitte volitamata isik, kes püüab leida paroole.
- Kasutajate jõudeolekut tuleks seirata ja rakendada parandusmeetmeid sõltuvalt jõudeperioodi pikkusest, näiteks blokeerida kasutajad 60-päevase jõudeaja järel ja kustutada kasutajad 90-päevase jõudeaja järel.
- Vaikekasutajate (näiteks külalise, administraatori, omaniku, juurkasutaja) ja allettevõtjate tegevust tuleks seirata iga päev. Soovitatav on selleks kasutada turbeinstrumente.
- Juurdepääs andmetele tuleks anda mingiks piiratud perioodiks päeva, nädal, kuu või aasta piires.

2.22 Juurdepääsu seire kaalutlusi

2.22.1 Kasutajate toimingute seire meetmed hõlmavad alljärgnevat.

- Seirata tuleks väga olulisi kontosid, logifaile, andmefaile ja andmebaase.
- Eeliskasutajate toimingute ja kasutajate nurjunud pääsukatsete seireks tuleks logid perioodiliselt läbi vaadata.
- Seirata tuleks meili kasutamist, sest meili kuritarvitused võivad tekitada õiguslikke, privaatsus- ja eetikaprobleeme.

G38 Pääsu reguleerimise meetmed (jätkub)

- Sisselogimise eeliskontode (süsteemikontode) kasutamist tuleks seirata ja põhjendada. Võimaluse korral peaksid sellistel kasutajatel olema oma logimisidentifikaatorid ja neile kinnistatud eelisõigused (süsteemiadministraatori konto); neil ei tohiks olla üldistatud identifikaatorit, sest seda võidakse kasutada ühiselt.

Tarnijailt saadud turvatooteid (näiteks võrku ja serverisse sissetungi avastamise vahendeid) ja nendega seotud logisid tuleks iga päev läbi vaadata ning alarme tuleks käsitleda asjakohaselt.

3 AUDITIPROTSESS

3.1 Plaanimine

3.1.1 Organisatsiooni riski kaalutlemise ja riskihaldusstrateegia põhjal tuleks koostada auditi kava, mis sisaldaks auditi käsitlusala, eesmärke ja ajastust. Auditi kavas tuleks selgelt dokumenteerida aruandluse korraldus. Tuleks arvestada organisatsiooni ja ta huvirühma iseloomu ja suurust. IS audiitor peaks endale selgeks tegema organisatsiooni missiooni ja tegevuseesmärgid, tehnilise infrastruktuuri tüübid ja tegevuse jaoks elutähtsad andmed.

3.1.2 Vaja on tunda organisatsiooni struktuuri, eriti aga olulise personali, sealhulgas teabe haldajate, omanike ja järelevalvajate rolle ja kohustusi.

3.1.3 Auditi plaanimisjärgu esmane eesmärk on tunda neid ohte ja riske, mis ähvardavad organisatsiooni siis, kui juurdepääsu määratletakse, kinnitatakse, määratakse, kasutatakse või reguleeritakse vääralt.

3.1.4 Läbivaatuse käsitlusala määratlemiseks nii, et rõhk oleks suure riskiga aladel, tuleks kasutada formaalseid riski kaalutlemise metoodikaid.

3.1.5 Võimaluse korral tuleks auditi plaanimisel mõelda testimistulemuste kvantiteerimiseks sobivatele valimivõtu meetoditele.

3.1.6 Kõik eelmised auditiaruanded tuleks läbi vaadata ja iga aspekti puhul hinnata lahendustaset vastavalt haldusmeetmete plaanile.

4 TÖÖ SOORITAMINE

4.1 Auditi tööd

4.1.1 IS audiitor peaks mõtlema alljärgneva läbivaatamisele:

- ülalnimetatud võimalike vältimis- ja avastusmeetmete järgimine;
- organisatsiooni skeem ja iga turbekohustustega töötaja ametijuhend;
- rollid, mis on seotud juurdepääsuga inforessurssidele (et teha kindlaks, kas nad on loodud kooskõlas praeguste tööülesannetega);

G38 Pääsu reguleerimise meetmed (jätkub)

- töötajate kontodele, sealhulgas infotehnoloogia grupiga seotud kontodele antud pääsuõigused (et teha kindlaks, kas neid kontrollitakse perioodiliselt veendumiseks, et üha on olemas tööalane vajadus);
- töösuhte lõpetanud töötajaile antud logimiskontod (et teha kindlaks, kas nad kõrvaldatakse niipea kui on võimalik);
- poliitikad, kriteeriumid ja protsesside teostused (et kontrollida asitõendeid täielikkuse, õigsuse, ajakohastuse ja vastavuse kohta);
- kinnitamise protseduur, kohustuste määratlemine ja nende aktsepteerimine turvalisusega seotud ülesannete puhul (näiteks: teabe omanikud, äriprotsesside omanikud, rakenduste omanikud);
- varade inventariloend koos liigituse ja riskihinnangutega;
- infoturbe administreerimise logid ja igapäevased meetmed, eriti eeliskasutajate puhul;
- turvaintsidentide avastamise, käsitluse laiendamise ja lahendamise protseduurid ja nende mõõdud läbivaadataval perioodil. Töötajate teadlikkuse hindamiseks turvaintsidentide protseduuride alal tuleks neid pisteliselt küsitleda;
- teadvustus- ja koolituskava ja sellega seotud mõõdustik;
- infoturbe administreerimise tööprotseduurid;
- asitõendid (kui need on olemas) läbivaadataval perioodil toimunud turvaintsidentidest teatamise, nende käsitluse laiendamise ja nende lahendamise kohta ning saadud õppetunnid ja kehtestatud tegevuskava;
- administraatori tegevuse põhjendus ja kinnitused ning tööalase kasutamise aluspõhimõtted;
- aruanded riski ja nõrkuste kaalutlemiste kohta;
- inimressursiprotseduuride osana (tavaliselt töösuhte alustamisel) allakirjutatud töölepingud ja sätted;
- ajutise personaliga sõlmitud lepingud;
- aruanded platvormide (näiteks serverite, lauaarvutite, hostide) konfiguratsioonide kohta;
- asitõendid läbivaadataval perioodil toimunud õiguste läbivaatuse protsessi kohta;
- aruanded tulemüüride ning sissetungi tuvastuse ja sissetungi tõrje süsteemide konfiguratsioonide kohta;
- tulemüüride ning sissetungi tuvastuse ja sissetungi tõrje süsteemide logid ühe punkti kohta;
- spetsiifilised standardid ja juhised (näiteks tulemüüri või veebirakenduste kohta);
- teenusetasemelepingud või -lepped ühiste või kolmandatest pooltest tarnijatega;

G38 Pääsu reguleerimise meetmed (jätkub)

5 ARUANDLUS

5.1 Aruande koostamine ja järeltoimingud

5.1.1 Auditiaruande kavand tuleks koostada ja läbi arutada koos asjassepuutuva personaliga. Aruandesse tuleb võtta ainult need aspektid, mida toetavad selged asitõendid.

5.1.2 Aruanne tuleks viimistleda ISACA suuniste järgi ja esitada juhtkonnale koos soovitustega täiustamise ja probleemide lahendamise ning järeltoimingute kohta.

5.1.3 Tuleks leppida kokku järeltoimingute, tegevuskavade, kohustuste, tähtaegade ning kõrgema juhtkonna määratavate ressursside ja prioriteetide kohta.

6 JÕUSTUMISKUUPÄEV

6.1 See suunis kehtib kõigi infosüsteemiauditite kohta alates 1. veebruarist 2008.

G39 IT korraldus

1 TAUST

1.1 Seos standarditega

1.1.1 Standard *S10 "IT ohje"* määrab: "IS audiitor peaks IS talituse läbi vaatama ja otsustama, kas see talitus on kooskõlas organisatsiooni missiooni, visiooni, väärtuste, eesmärkide ja strateegiatega. IS audiitor peaks kontrollima, kas IS talitusel on selge määrang soorituse (toimivuse ja tõhususe) kohta, mida ootab organisatsiooni talitlus, ja hindama ta tulemusi."

1.2 Seos COBITiga

1.2.1 PO1 *"Määratleda strateegiline IT plaan"* määrab:"IT-le esitatavat äristrateegia säilitamise või laiendamise ärinõuet ja haldusnõudeid rahuldav ning tulude, kulude ja riskide suhtes läbipaistev strateegilise IT-plaani määratlemise IT-protsessi juhtimine saavutatakse keskendumisega IT ja talitluse halduse lülitamisele ärinõuete muundamisse teenusepakkumusteks ning strateegiate väljatöötamisele nende teenuste läbipaistvaks ja toimivaks tarnimiseks."

1.2.2 PO4 *"Määratleda IT protsessid, organisatsioon ja seosed"* määrab: "IT-le esitatavat äristrateegiale kiire reageerimise ärinõuet rahuldav ja suunavatele nõuetele vastav ning määratletud ja pädevaid kokkupuutepunkte tagav IT protsesside, organisatsiooni ja seoste määratlemise IT-protsessi juhtimine saavutatakse keskendumisega läbipaistvatele, paindlikele ja reageerimisvõimelistele IT organisatsiooniliste struktuuride rajamisele ning IT-protsesside määratlemisele ja teostamisele, nii et omanikud, rollid ja kohustused integreeritakse talitlus- ja otsustusprotsessidesse."

1.2.3 PO5 *"Hallata IT-investeeringuid"* määrab: "IT-le esitatavat kuluefektiivsuse pideva ja tõendatava kasvu ning äritegevuse kasumlikkusesse lõppkasutaja ootustele vastavate integreeritud ja standardsete teenustega panuse andmise ärinõuet rahuldav IT-investeeringute haldamise IT-protsessi juhtimine saavutatakse keskendumisega toimivatele ja tõhusatele otsustustele IT-investeerimise ja -portfelli kohta ning IT-eelarvete joondamisega IT-strateegiat ja -investeeringuid puudutavate otsuste järgi ja nende eelarvete jälgimisega."

1.2.4 SH4 *"Tagada IT haldus"* määrab: "IT-le esitatavat organisatsiooni halduse eesmärkide ja IT halduse integreerimise ärinõuet rahuldav ning õigusnormidele vastav IT halduse tagamise IT-protsessi juhtimine saavutatakse keskendumisega aruannete koostamisega juhatusele IT strateegia, tulemuste ja riskide kohta ning reageerimisega haldusnõuetele kooskõlas juhatuse suunistega."

1.2.5 Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ning arvestades COBITi juhtimiseesmärke ja nendega seotud haldustavasid. IS audiitorile õiguste, kohustuste ja vastutuse kohta esitatavate nõuete täitmiseks on alljärgnevas need COBITi protsessid, mille asjakohasus, valimine ja rakendamine on kõige tõenäolisem, jagatud esmasteks ja teisejärgulisteks. Protsess ja juhtimiseesmärgid, mis tuleb valida, võivad varieeruda sõltuvalt ülesande lähtetingimustest.

1.2.7 Käesoleva suunisega käsitletava ala läbivaatusel tuleks teises järjekorras arvestada järgmisi spetsiifilisi COBITi eesmärke või protsesse:

- PO2 – Määratleda infoarhitektuur;
- PO3 – Määratleda tehnoloogiline suund;
- PO6 – Teavitada juhtimissihid ja suund;
- PO7 – Hallata IT inimressursse;
- PO8 – Hallata kvaliteeti;
- PO9 – Hinnata IT riskid ja hallata neid;
- PO10 – Hallata projekte;
- TT1 – Määratleda teenusetasemed ja hallata neid;
- TT2 – Hallata kolmandate poolte teenuseid;
- TT3 – Hallata suutlikkust ja võimsust;
- TT6 – Tuvastada ja kinnistada kulud;
- TT7 – Koolitada kasutajaid;
- TT8 – Hallata konsultatsioonipunkti ja intsidente;
- TT9 – Hallata konfiguratsiooni;
- TT10 – Hallata probleeme;
- TT12 – Hallata füüsilist keskkonda;
- TT13 – Hallata käitust;
- HE2 – Hankida rakendustarkvara ja hooldada seda;
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda;
- HE6 – Hallata muutusi;
- SH1 – Seirata ja hinnata IT töötulemusi.

1.2.8 IT korralduse seisukohalt kõige asjakohasemad teabekriteeriumid on

- esmajärjekorras: toimivus ja tõhusus;
- teises järjekorras: konfidentsiaalsus, käideldavus, terviklus, vastavus ja usaldatavus.

1.3 Suunise eesmärk

1.3.1 Struktuur võib olla organisatsiooni toimivuse ilmne võimaldaja või pidurdaja, kuid pelgalt struktuur ei otsusta organisatsiooni edu. Pole olemas mingit ainuõiget struktuuri, sest ükski organisatsioon ei sarnane täpselt teisele. Kõigil IT organisatsioonidel on sarnased eesmärgid ja sarnane vastutus, kuid nende profiilid, haldussüsteemid, protsessid, kitsendused ning tugevad ja nõrgad küljed teevad igast IT organisatsioonist ainulaadse. On siiski teatavad atribuudid, millega kontrollida IT organisatsioonilise struktuuri optimaalsust.

1.3.2 See suunis annab juhiseid IS auditeerimise standardi S10 "IT ohje" rakendamise kohta. IS audiitor peaks seda suunist arvestama otsustamisel, kuidas jõuda ülalnimetatud standardi rakendamiseni, kasutama selle rakendamisel kutsealast otsustusvõimet ning olema valmis põhjendama iga lahknevust.

1.4 Suunise rakendamine

1.4.1 Selle suunise rakendamisel peaks IS audiitor arvestama teda seoses muude asjassepuutuvate ISACA standardite ja suunistega.

2 IT ORGANISATSIOON

2.1 Organisatsioonide tüübid

2.1.1 Praeguste organisatsioonide piirid on paindlikumad ja dünaamilisemad ning enamasti laiemad. Organisatsioonid ja majandusharud mõistavad, et neil tuleb hakata keskenduma tervetele protsessidele, sealhulgas sellistele, mis ulatuvad organisatsiooni füüsilistest seintest väljapoole. Neil tuleb sirutuda oma äripartnerite, tarnijate ja klientideni. Täpne, sobiv ja õigeaegne teave on uue majanduse ja niinimetatud avardatud ettevõtte vältimatu koostisosa. Avardatud ettevõtte huvipoolte vahelise teabe ja teadmuse jagamise tegevus on üks keskseid edutegureid toimiva ettevõttehalduse loomiseks. Üldine konkurentsistrateegia peab olema toimiva teadmiste halduse strateegia ja suunamise tõukejõud. Organisatsioon peab rajama sobiva teabekorralduse kõrgemale juhtkonnale otsustusteks vajaliku teabe andmiseks ning seda sobival määral reguleerima.

2.2 Kooskõla

2.2.1 IT ning äritegevuse ja kõigi selle komponentide kooskõla maksimeerimiseks pole mingit universaalset metoodikat. Paljugi sõltub ettevõtte iseloomust, suurusest, turgudest, IT-sõltuvusest, juhtimisstiilist ja kultuurist. Peale selle mõjutavad organisatsiooni kooskõla komponente ja struktuuri ka sisemised IT-võimed, sõltuvus väljasttellimisest, väljasttellimise iseloom ja üldine halduse struktuur.

2.2.2 Viimastel aastatel on IT hakanud senisest peamiselt sisemise talitluse toetajast muutuma kogu äritegevuse esmaseks soodustajaks ja võimaldajaks. Kui ettevõttel ei ole õiget kooskõla IT-ga, pole tõenäoline, et see ettevõte saavutaks edu väärtuse andmisel oma huvipooltele ja oleks pikemat aega edukas. IT kooskõla ettevõte üldise strateegiaga ei teki juhuslikult. Ta nõuab ettevõtte paljude tasemete ja tegevuste täielikku ja aktiivset osalust ning aktiivset ja keskendunud juhtimist. See on pidev pingutus ning nõuab maailmaklassi oskusi ja asjatundmist, olgu see sisemine või väljastpoolt tellitud. Lisaks tugevale ja tõendatavale suunamisele on vaja ka riskida, kuid rakendades asjakohast riskihaldust.

2.2.3 IT kooskõla õige suunamine nõuab ettevõtte kõige kõrgematelt tasemetelt eestvedajaks olemist ja pühendumist. Selleks peavad tegevjuhataja ja juhatus osalema ettenägelikult. Juhatus peab selleks võtma endale kohustuse

- tagada IT strateegia kooskõla äristrateegiaga;
- tagada, et IT tegevus järgiks seda strateegiat;
- suunata IT strateegiat investeeringute sobivaks tasakaalustamiseks süsteemide vahel, mis toetavad ettevõtet ta senisel kujul, muundavad ettevõtet või arendavad ettevõtet.

2.3 IT strateegiline plaan

2.3.1 Organisatsioon peaks rajama juhatuse tasemel IT strateegia komisjoni. See komisjon peaks kontrollima, kas IT haldusega kogu organisatsiooni halduse osana tegeldakse adekvaatselt, andma nõu strateegilise suuna kohta ja kogu juhatuse nimel vaatama läbi suuremad investeeringud.

2.3.2 IT strateegia komisjon peaks koostama IT strateegilise plaani, mis koostöös asjassepuutuvate huvipooltega määratleks, milline on edaspidi IT osa ettevõtte strateegilistes eesmärkides (sihtides) ning nendega seotud kuludes ja riskides. Ta hõlmab seda, kuidas toetab IT edaspidi IT-ga võimaldatavaid investeerimiskavasid ja kasutuskõlblike teenuste andmist. Plaan määratleb, kuidas eesmärke saavutatakse ja mõõdetakse, ning saab huvipooltelt formaalse kinnituse. IT strateegiline plaan peaks käsitlema investeerimise ja käituse eelarvet, rahastusallikaid, allikate strateegiat, hankimise strateegiat ning õigusaktide nõudeid.

2.3.3 Strateegiline plaan peaks olema piisavalt detailne võimaldamaks määratleda taktikalisi IT-plaane. Tuleks luua IT strateegilisest plaanist tuletatavate taktikaliste IT-plaanide portfell. Need taktikalised plaanid kirjeldavad vajalikke IS-üritusi, ressursivajadusi ning seda, kuidas hakatakse ressursside kasutamist ja hüvede saavutamist seirama ja haldama. Taktikalised plaanid peaksid olema piisavalt detailsed võimaldamaks määratleda projektiplaane. Kehtestatud taktikalisi IS-plaane ja üritusi tuleks aktiivselt hallata projekti- ja teenuseportfellide analüüsi kaudu. Harilikult hõlmab see regulaarset nõuete ja ressursside tasakaalustamist, nende võrdlemist strateegiliste ja taktikaliste sihtide ja oodatavate hüvede saavutamisega ning asjakohaste meetmete rakendamist lahknevuste korral.

2.4 IT suunamise komisjon

2.4.1 Tuleks rajada tegev-, äri- ja IT-juhtidest koosnev IT suunamise komisjon (või sellele vastav organ), kes peaks

- määrama IT-ga võimaldatavate investeerimiskavade prioriteedid kooskõlas ettevõtte äristrateegia ja prioriteetidega;
- jälgima projektide seisu ja lahendama ressursikonflikte;
- seirama teenusetasemeid ja teenuste täiustamist.

G39 IT korraldus (jätkub)

2.4.2 Strateegia rakendamise järelevalvaja rollis oleva IT suunamise komisjoni liikmete hulgas peaks olema vähemalt üks juhatuse liige (komisjoni esimees) ning teda peaksid abistama põhi- ja abitegevuse osakondade juhatajad, peainformaatik ja peatehnoloog (või sellele vastav) ning muud olulise panuse andjad, sealhulgas õigus-, auditi-, rahandusalased jt. Komisjon peaks asju arutama detailsemalt kui IT strateegia komisjon ning ta peaks andma suure osa lähteandmetest strateegiakomisjoni üldisemateks aruteludeks, näiteks andes soovitusi alljärgnevates küsimustes:

- IT-kulutuste iga-aastane tase;
- ettevõtte IT arhitektuuri kooskõla ärieesmärkidega;
- portfellihaldus, sealhulgas suurte It-ga seotud äriinvesteeringute projektiplaanide kinnitamine;
- projektiplaanide seire ja kontrollimine, kas sisemised ja välised muutused on ajakohastatud plaanides sobivalt arvesse võetud;
- IT-ga seotud ressursside soetamine ja loovutamine;
- IT-ressursse puudutavate konfliktide seire selgelt sõnastatud äriprioriteetide põhjal;
- strateegiliste sihtide teatavakstegemine projektirühmadele asjassepuutuvate allüksuste esindajate kaudu;
- mõõtmisplaanide sõnastamine ja IT mõõdikupaneeli, IT tasakaalus tulemuskaardi või muu olulise mõõdustikuga saadud tulemuste ülevaatus;
- IT väärtuse selgitamine kõigile huvipooltele. Seda võib teha organisatsiooni sisevõrgus või siseväljaannetes ilmuvate artiklitega, tähtsam aga on seda selgitada huvigruppidele ja välistele vaatlejatele organisatsiooni veebisaidi kaudu või huvigruppide teabekanalite kaudu.

2.5 IT-talituse ja abitalituste koht organisatsioonis

2.5.1 IT-talitus peaks paiknema organisatsiooni üldstruktuuris vastavalt talitlusmudelile, mis sõltub IT tähtsusest ettevõttes. Konkreetsemalt, tuleks arvestada ta elulist tähtsust äristrateegiale ja tegutsemise IT-st sõltuvuse taset. Peainformaatiku alluvusliin peaks olema proportsioonis IT tähtsusega ettevõttes ja potentsiaalsete IT-lt saadavate hüvedega.

2.6 Organisatsiooniline struktuur

2.6.1 Tuleks rajada sisemine ja väline IT organisatsiooniline struktuur, mis kajastaks ärivajadusi. Peale selle peaks olema kasutusel protsess IT organisatsioonilise struktuuri perioodiliseks läbivaatuseks, et korrigeerida personalivajadusi ja soetamisstrateegiaid eeldatavate ärieesmärkide ja muutuvate tingimustega kohandamiseks.

2.6.2 IT organisatsiooni määratlemisel tuleks arvestada nõudeid personali, oskuste, funktsioonide, vastutuse, õiguste, kohustuste, rollide ja kohustuste ning järelevalve kohta. See organisatsioon peaks olema ehitatud mingisse IT-protsesside raamstruktuuri, mis kontrollib läbipaistvust ja juhtimist ning ka kõrgemate juhtide ja ettevõtte juhtkonna osalemist.

2.6.3 IT strateegia komisjon peaks kontrollima juhatuse IT-haldust ning üks või mitu suunamiskomisjoni, kus osalevad põhitegevus ja IT, peaks määrama IT-ressurssidele prioriteetide andmise kooskõlas ärivajadustega. Kõigis talituste jaoks peaksid olema kasutusel protsessid, administreerimispoliitikad ja protseduurid, mis pööravad tähelepanu eriti juhtimisele, kvaliteedi tagamisele, riskihaldusele, infoturbele, andmete ja süsteemide omandusele ja kohustuste lahususele. Ärinõuete õigeaegse toetamise kontrollimiseks tuleks IT lülitada asjassepuutuvatesse otsustusprotsessidesse.

2.6.4 IT strateegilise plaani elluviimiseks peaks olema kasutusel mingi IT-protsesside raamstruktuur. See raamstruktuuriga tuleks hõlmata IT-protsesside struktuur ja seosed (näiteks protsesside lünkade ja ülekatete halduseks), omandus, küpsus, soorituse mõõtmine, täiustamine, vastavus, kvaliteedieesmärgid ja nende saavutamise plaanid. Ta peaks tagama integratsiooni IT-spetsiifiliste protsesside, ettevõtte portfellihalduse, äriprotsesside ja äritegevuse muutmise protsesside vahel. IT-protsesside raamstruktuur peaks olema integreeritud kvaliteedihalduse süsteemiga ja sisejuhtimise raamstruktuuriga.

2.7 Rollid ja kohustused

2.7.1 Tuleks määratleda ja teatavaks teha organisatsiooni kõigi töötajate rollid ja kohustused IS suhtes, tagades piisavad õigused rolli ja sellega seotud kohustuste täitmiseks. Need kirjeldused peaksid detailselt näitama õigusi ja kohustusi, sisaldama kõnealustel ametikohtadel nõutavate oskuste ja kogemuste määratlusi ning sobima sooritusе hindamise tarbeks.

2.8 IT kvaliteedi tagamise kohustused

2.8.1 Tuleks määrata kohustused kvaliteedi tagamise ülesande täitmise alal ning luua kvaliteedi tagamise grupp, kellel on sobivad oskused kvaliteedi tagamise süsteemide, meetmete ja teavituse alal. Kvaliteedi tagamise grupi koht organisatsioonis, ta kohustused ja ta suurus peaksid rahuldama organisatsiooni vajadusi.

2.9 Protsesside väljasttellimine

2.9.1 Enamikus ettevõtetes läheb suur osa IT-kulutustest käitusele ja kasutajate toele. Neid teenuseid saavad küll anda ka ettevõtete endi IT-osakonnad, kuid tippjuhtidele on üha enam selge, et nii kohalikud kui ka välismaised teenuseandjad pakuvad väärtust ja sageli distsiplineeritumat lähenemist klienditeenindusele.

2.9.2 Koos IT strateegilise tähtsuse kasvuga on kasvanud tippjuhtide ootused IT suhtes. Sellise olukorra tõttu on tekkinud uusi ja loovaid väljasttellimise kasutusalasid, mis hoiavad tasakaalu sisemise organisatsiooniga. Paljudel juhtudel jääb sisemise IT-organisatsiooni hooleks igapäevaste teenuste andmine, näiteks kasutajate abistamine, andmetöötluskeskuse käitus ja rakenduste väljatöötamine, panus strateegiasse või uuenduse juhtimine jäetakse aga välistele konsultantidele (seda võib pidada spetsialiseerituks ja paindlikuks). Töö toetamise reguleerimise kasvu tõttu võivad neid tendentse mõnikord toetada tippjuhid. Kuna IT-süsteemide vahetamine võtab aega, kasvab IT-organisatsioonile langevate vastavuse puuduste osakaal, halvendades neid tendentse ja keskendudes nende küsimuste lahendamiseks veel enam sisemistele ressurssidele. Tippjuhid mõistavad IT strateegilist kasutamist puudutavate nõuannete vajadust ja kui nad ei saa neid IT-organisatsioonilt, otsivad nad neid mujalt. Kolmandatest pooltest tarnijate ja konsultantide kasutamisel nõuannete saamiseks võidakse riskida objektiivsuse puudumisega, sest nad võivad soovitada nii strateegiliseks kui ka rutiinseks otstarbeks omaenda tooteid ja teenuseid. Kui IT-organisatsioon ei saa anda strateegilist nõu, võib ta kaotada ka võimaluse anda rutiinseidki teenuseid. Protsesside väljasttellimine võib tuleneda ka juhtkonna otsusest keskenduda oma põhitegevustele ning ka sellest, et IT-protsessi väljasttellimine on ökonoomsem kui sisemise asjatundmise kasutamine.

2.10 IT infrastruktuur ja arvutite käitus

2.10.1 Täielik ja õige andmetöötlus nõuab toimivat andmetöötluse ja riistvarahoolduse haldust. See protsess sisaldab käituse poliitikate ja protseduuride määratlemist plaanilise töötluse, tundlike väljundandmete kaitse, infrastruktuuri seire ja riistvara profülaktilise hoolduse toimivaks halduseks. Toimiv käituse haldus aitab säilitada andmete terviklust ning vähendab hilistusi põhitegevuses ja IT käituskulusid.

2.10.2 Arvutiseadmete ja -personali kaitse nõuab hästikavandatud ja hästihallatud füüsilisi rajatisi. Füüsilise keskkonna halduse protsess hõlmab füüsilisele asukohale esitatavate nõuete määratlemist, sobivate rajatiste valimist ning toimiva protsessi kavandamist keskkonnategurite seireks ja füüsilise juurdepääsu halduseks. Toimiv füüsilise keskkonna haldus vähendab arvutiseadmete ja personali kahjustamisest tingitud katkestusi põhitegevuses. Seadmete normaalset tööd aitab tagada ka hea profülaktilise hoolduse ajakava.

2.10.3 Riistvara ja tarkvara konfiguratsioonide tervikluse kontroll nõuab täpse ja täieliku konfiguratsioonihoidla rajamist ja hooldamist. See protsess hõlmab teabe kogumist algsete konfiguratsioonide kohta, alusvariantide kehtestamist, konfiguratsiooniteabe kontrollimist ja auditeerimist ning vajaduse korral konfiguratsioonihoidla ajakohastamist. Toimiv konfiguratsioonihaldus soodustab süsteemide käideldavuse kasvu, minimeerib tootmisprobleeme ja lahendab neid probleeme kiiremini.

2.10.4 Kiire ja toimiv reageerimine IT kasutaja küsimustele ja probleemidele nõuab hästikavandatud ja hästi sooritatavat hoolduspunkti ja intsidendihalduse protsessi. See protsess sisaldab hoolduspunkti talituse rajamist registreerimiseks, intsidendikäsitluse laiendamiseks, tendentside ja algpõhjuste analüüsiks ja probleemide lahendamiseks. Ärilisi hüvesid annab tööviljakuse kasv kasutajate küsimuste kiirema lahendamise

tõttu. Peale selle võib ettevõte käsitleda algpõhjusi (näiteks kasutajate halba koolitust) toimiva aruandluse kaudu.

2.10.5 Pidevate IT-teenuste andmise vajadus nõuab IT jätkusuutlikkuse plaanide koostamist, käigushoidu ja testimist, varukoopiate hoidmist teises asukohas ning perioodilisi õppusi jätkusuutlikkuse plaani alal. Toimiv pideva teenuse protsess minimeerib suuremate IT-teenuse katkestuste tõenäosust ja toimet ettevõtte kesksetes talitlusfunktsioonides ja -protsessides.

2.10.6 Vajadus hallata IS-ressursside sooritust ja suutvust nõuab protsessi, millega IS-ressursside soorituse ja suutvuse hetkeseisu perioodiliselt läbi vaadata. See protsess sisaldab tulevaste vajaduste prognoosimist töökoormust, salvestust ja ootamatuste käsitlust puudutavate nõuete põhjal. See protsess annab kinnitust sellel, et ärivajadusi toetavad inforessursid on pidevalt saadaval.

2.10.7 Vajalikke teenuseid puudutavat toimivat suhtlust IS juhtkonna ja äriklientide vahel võimaldavad IS-teenuste ja teenusetasemete dokumenteeritud määratlus ja lepe. See protsess sisaldab ka seiret ja õigeaegset huvipoolte teavitamist teenusetasemete seisust. See protsess võimaldab hoida IS-teenused kooskõlas nendega seotud ärinõuetega.

2.11 Käitusprotseduurid ja -tööd

2.11.1 IT käituseks peaksid olema määratletud, rakendatud ja käigus hoitavad tüüpsed protseduurid ning käituspersonal peaks tundma talle määratud töid. Pideva käituse tagamiseks peaksid käitusprotseduurid hõlmama vahetuste üleandmist (st tegevuse formaalset üleandmist, olekute ajakohastust, käitusprobleeme, käsitluse laienduse protseduure, aruandeid hetkekohustuste kohta). Määratletud peaksid olema ka protseduurid IT infrastruktuuri ja sellega seotud sündmuste seireks.

2.12 Rakenduste arendus

2.12.1 Rakendussüsteemide soetamiseks või väljatöötuseks on mitu võimalust, sealhulgas järgmised:

- individuaalne väljatöötus sisemiste ressurssidega;
- individuaalne väljatöötus osaliselt või täielikult väliste ressurssidega (mis võivad olla kohalikud või kaugemad);
- tarnija tarkvarapaketid, mida rakendatakse muudatusteta;
- tarnija tarkvarapaketid, mida rakendatakse erinõuete täitmiseks kohandatult.

Mõnikord võivad suured ja keerukad rakendused (mis võivad sisaldada ettevõtte ressursside plaanimise süsteeme) kujutada endast ülaloetletu kombinatsiooni.

G39 IT korraldus (jätkub)

2.13 Lepingu järgimine väljasttellimist kasutavas IT-talituses

2.13.1 Suur hulga IT-teenuseid (alates IT konsultatsioonipunktist ja lõpetades IT käitusega) saab tellida kolmandatest pooltest tarnijatelt. Vajadus kindlustada kolmandatelt pooltelt saadavate teenuste vastavus ärinõuetele nõuab toimivat kolmandate poolte halduse protsessi. Selle protsessiga määratletakse kolmandate pooltega sõlmitavates kokkulepetes selgelt rollid, kohustused ja ootused ning sooritatakse selliste kokkulepete läbivaatusi ja seiret nende toimivuse ja vastavuse vaatepunktist. Toimiv kolmandate poolte teenuste haldus minimeerib äririski, mis on seotud tarnijate suutmatusega.

2.14 Kolmandate poolte käsitluse protseduurid

2.14.1 Kõik kolmandatest pooltest tarnijate teenused tuleks identifitseerida ja liigitada tarnija tüübi, olulisuse ja elutähtsuse järgi. Rolle, kohustusi, eesmärke ja eeldatavaid tarneobjekte hõlmav tehniliste ja organisatsiooniliste suhete formaalne dokumentatsioon peaks sisaldama neid tarnijaid esindavate isikute volitusi. Iga kolmandast poolest tarnijaga suhtlemise halduse protsess tuleks formaliseerida. Suhte omanikud peavad pidama sidet klientuuri küsimustes ning kindlustama usaldusel ja läbipaistvusel põhineva suhte kvaliteeti näiteks teenusetasemelepetega (SLA). Kui hakatakse teenust saama uuelt kolmandapoolselt tarnijalt, tuleks kaaluda teenusetarnija võimet täiendada ja sobitada oma teenuseid äritegevuse muudatuste korral.

2.14.2 Teenuse tarnimise seireks tuleks rajada protsess, millega kontrollida, kas tarnija rahuldab praegusi ärinõudeid ja endiselt järgib lepingusätteid ja teenusetasemeleppeid, ning kas ta tulemused on konkurentsivõimelised alternatiivsete tarnijate hulgas ja teistsugustes turutingimustes.

2.15 Kohustused riski, turvalisuse ja vastavuse alal

2.15.1 Omandus ja kohustused IT-ga seotud riskide alal peaks olema põhitegevuse lahutamatu osa mingil sobival kõrgemal tasemel. Peaksid olema määratletud ja määratud elutähtsate IT-riskide halduse rollid, sealhulgas spetsiifiliste kohustustega infoturbe, füüsilise turbe ja vastavuse alal. Üleorganisatsiooniliste küsimuste käsitlemiseks tuleks kehtestada riski- ja turbehalduse kohustused ettevõtte tasemel. Võib-olla on vaja määrata turbehalduse lisakohustused süsteemispetsiifilisel tasemel, süsteemiga seotud turvaküsimuste käsitlemiseks. Kõrgem juhtkond peaks andma nõupidamiste kaudu suuniseid ja juhtnööre IT-riski talumise ja IT-jääkriskide aktsepteerimise kohta.

2.16 Personali palkamine ja säilitamine

2.16.1 Personalitarvet tuleks hinnata regulaarselt või äri-, talitlus- või IT-keskkonna suuremate muutuste puhul, kontrollides, kas IT-talitusel on piisav arv pädevaid IT-töötajaid. Personali komplekteerimine peaks arvestama põhitegevus- ja IT-personali talituseülese koolituse ühitamist, töökohtade rotatsiooni ja väljasttellimise võimalusi.

G39 IT korraldus (jätkub)

2.16.2 Tuleks määratleda ja välja selgitada kesksed IT-töötajad ning minimeerida ülemäärane sõltuvus neist. Peaks olema kehtestatud plaan kesksete IT-töötajatega ühendusseastumiseks hädaolukorras. Tuleks ka määratleda ja kehtestada poliitikad ja protseduurid, millega IT-talitus reguleeriks konsultantide ja muu lepingulise personali tegevust, nii et tagataks organisatsiooni varade kaitse ja kokkulepitud lepingunõuete täitmine. Need peaksid sisaldama keskseid soorituse näitajaid, mis aitaksid kontrollida, kas personali töötulemused vastavad ootustele.

3 AUDITIPROTSESS

3.1 Plaanimine

3.1.1 Organisatsiooni riski kaalutlemise ja riskihalduse strateegia põhjal tuleks välja töötada auditi kava, mis hõlmaks auditi käsitlusala, eesmärke ja ajastust. Auditi kavas tuleks selgelt dokumenteerida aruandluse korraldus. Tuleks arvestada organisatsiooni ja ta huvigruppide iseloomu ja suurust. IS audiitor peaks omandama ettekujutuse organisatsiooni missioonist ja ärieesmärkidest, tehnilise infrastruktuuri tüüpidest ja põhitegevuse jaoks elutähtsatest andmetest.

3.1.2 Läbivaatuse käsitlusala määratlemiseks tuleks kasutada riski kaalutlemise metoodikaid, keskendudes suure riskiga aladele.

3.1.3 Tuleks läbi vaadata kõik eelmised auditiaruanded ja hinnata juhtkonna tegevusplaani alusel iga küsimuse lahenduse taset.

3.1.4 IS audiitor peaks hankima IT-korralduse kohta teavet, sealhulgas järgmised andmed:

- olulise personali, seahulgas teabe juhtide, omanike ja järelevalvajate rollid ja kohustused;
- kõrgema juhtkonna suunamisrollid ja -kohustused;
- organisatsiooni eesmärgid ning pika- ja lühitähtajalised plaanid;
- ettevõtte strateegiliste suundade seadmine;
- IT eesmärgid ning pika- ja lühitähtajalised plaanid;
- aruanded hetkeseisu kohta ja plaanimis- või suunamiskomisjoni koosolekute protokollid;
- teabe arhitektuuri mudel;
- IT korraldust ja seoseid käsitlevad poliitikad ja protseduurid;
- ametijuhendid, koolitus- ja arenguandmikud;
- lepingud kolmandatest pooltest teenuseandjatega;
- andmed selle kohta, kas ettevõte on välja arendanud talle seatud strateegiliste sihtide saavutamiseks vajalikud oskused ja IT infrastruktuuri.

3.1.5 IS audiitor peaks välja selgitama ja endale üldjoontes selgeks tegema protsessid, mis võimaldavad IT-organisatsioonil täita ülesandeid, mis on loetletud jaotises 4.1.1, sealhulgas hoida käigus sidekanaleid, mille kaudu seatakse sihte ja eesmärke madalamatele tasemetele (laskuva suunaga) ja edastatakse teavet vastavuse seire kohta (üleneva suunaga).

3.1.6 IS audiitor peaks hankima teavet (dokumenteeritud või muud) organisatsiooni IS-strateegia kohta, sealhulgas järgmist:

- lühi- ja pikatähtajalised plaanid organisatsiooni missiooni täitmiseks ja sihtide saavutamiseks;
- IT ja süsteemide lühi- ja pikatähtajalise strateegia ja plaanid ülalnimetatud plaanide toetuseks;
- metoodika IT strateegia seadmiseks, plaanide koostamiseks ja edenemise seireks nende plaanide alusel;
- metoodika IT strateegia ja plaanide muudatuste reguleerimiseks;
- IT missiooni määrang ning IT-tegevuste kokkulepitud sihid ja eesmärgid;
- hinnangud praeguste IT-tegevuste ja -süsteemide kohta.

3.2 IS auditi eesmärgid

3.2.1 IT-organisatsiooni auditi eesmärke võivad mõjutada sihtlugejaskonna vajadused ja kavatsetav levitamistase. Auditi üldiste eesmärkide püstitamisel peaks IS audiitor mõtlema järgmistele küsimustele:

- aruandlus IT-organisatsiooni ja/või ta toimivuse kohta;
- kas IT-üritused toetavad organisatsiooni missiooni ja sihte;
- rakenduste, tehnoloogia ja organisatsiooni alternatiivsete strateegiate hindamine.

3.2.2 IT-organisatsiooni IS auditi detailsed eesmärgid sõltuvad harilikult sisejuhtimise raamstruktuurist, mida kasutab tippjuhtkond. Mingi väljakujunenud raamstruktuuri puudumisel tuleks detailsete eesmärkide seadmise minimaalse alusena kasutada COBITi raamstruktuuri.

3.3 Auditi käsitlusala

3.3.1 IS audiitor peaks võtma auditi käsitlusalasse asjakohased IT-tegevuse plaanimise ja organiseerimise protsessid ja selle tegevuse seire protsessid.

3.3.2 Auditi käsitlusala peaks hõlmama juhtimissüsteeme kõigi COBITi raamstruktuuris määratletud IT-ressursside kasutamiseks ja kaitseks. Nende ressursside hulka kuuluvad

- andmed,
- rakendussüsteemid,

- tehnoloogia,
- rajatised,
- inimesed,
- IT haldus.

3.4 Personal

3.4.1 IS audiitor peaks saama mõistliku kinnituse sellele, et selle läbivaatuse sooritamiseks kasutataval personalil on sobiv ametiaste ja pädevus.

4 AUDITITÖÖ SOORITAMINE

4.1 IT organisatsiooni ja strateegilise plaanimise protsessi läbivaatus

4.1.1 IT organisatsiooni ja seoste läbivaatamisel peaks IS audiitor mõtlema sellele, kas IT organisatsioonil on õige personali ja oskuste kombinatsioon ning kas rollid ja kohustused on määratletud, teatavaks tehtud ja viidud kooskõlla põhitegevusega. IS audiitor võib läbivaatusel kontrollida, kas

- poliitikate sõnastused ja kõrgema juhtkonna avaldused tõendavad IT-talituse sõltumatust ja õigusi;
- IT plaanimis- või suunamiskomisjoni liikmesus ja ülesanded on määratletud ja kohustused piiritletud;
- IT plaanimis- või suunamiskomisjoni põhikiri seab komisjoni sihid kooskõlla organisatsiooni eesmärkidega ja lühi- ja pikatähtajaliste plaanidega ning IT eesmärkidega ja lühi- ja pikatähtajaliste plaanidega;
- peainformaatiku alluvusliin on proportsioonis IT-talituse tähtsusega ettevõtte tegevusele ning järgib tendentse ettevõtte tegevusalal ja ettevõtte turul;
- poliitikad käsitlevad organisatsiooni struktuuri hindamise ja muutmise vajadust muutuvate eesmärkide ja tingimuste puhuks;
- kõrgem juhtkond kontrollib rollide ja kohustuste täitmist;
- on olemas poliitikad, mis visandavad organisatsiooni kõigi töötajate rollid ja kohustused infosüsteemide, sisejuhtimise ja turbe alal;
- IT-organisatsiooni jaoks on olemas kvaliteedi tagamise talitus ja poliitikad;
- kõigi peamiste andmeallikate ja süsteemide jaoks on olemas poliitikad, mis hõlmavad andmete ja süsteemide omandust;
- on olemas poliitikad ja protseduurid, mis kirjeldavad järelevalve tavasid, millega kontrollida, kas rolle ja kohustusi täidetakse asjakohaselt ning kas kogu personalil on oma rollide ja kohustuste täitmiseks piisavad õigused ja ressursid;

G39 IT korraldus (jätkub)

- on olemas kohustuste lahusus süsteemide arenduse ja hoolduse vahel, süsteemide arenduse ja käituse vahel, süsteemide arenduse või hoolduse ja infoturbe vahel, käituse ja andmeohje vahel, käituse ja kasutajate vahel ning käituse ja infoturbe vahel;
- säilitatakse IT personali komplekteeritus ja pädevus, tagades ta võime luua toimivaid tehnoloogialahendusi;
- oluliste protsesside, sealhulgas süsteemiarenduse elutsükli tegevuste, infoturbe, hankimise ja suutvuse plaanimise puhul on olemas rollid ja kohustused;
- IT-talituse tulemuste mõõtmiseks organisatsiooni eesmärkide saavutamise alal kasutatakse sobivaid ja toimivaid keskseid soorituse indikaatoreid ja/või kriitilisi edutegureid;
- on olemas IT-poliitikad ja -protseduurid konsultantide ja muude lepinguliste töötajate tegevuse reguleerimiseks ning seega organisatsiooni varade kaitse kindlustamiseks;
- väljasttellitavatele IT-teenustele rakendatakse protseduure, mis taotlevad teenuste adekvaatsust ja vastavust organisatsiooni hankepoliitikatele;
- on olemas protsessid, millega koordineerida, teha teatavaks ja dokumenteerida huvisid IT-talituses ja väljaspool seda;
- on kasutusel poliitikad ja protseduurid, millega tagada, et IT-talituselt saadavate teenuste maksumus on põhjendatud ja on kooskõlas maksumustega sellel tegevusalal;
- organisatsiooni palkamis- ja vallandamisprotseduurid sisaldavad taustakontrolli.

4.1.2 IT strateegilise plaanimise protsessi läbivaatamisel peaks IS audiitor mõtlema sellele, kas

- on olemas IT missiooni ja nägemuse selge määratlus;
- on kasutusel mingi IT strateegilise plaanimise metoodika;
- see metoodika seob põhitegevuse sihid ja eesmärgid IS talitluse sihtide ja eesmärkidega;
- seda plaanimisprotsessi ajakohastatakse perioodiliselt (vähemalt kord aastas;
- see plaan piiritleb suuremad ettevõtmised IT alal ja vajalikud ressursid;
- selles protsessis osalevate isikute tase on sobiv.

4.1.3 Praeguse süsteemide portfelli administreerimiseks kasutatavate protsesside läbivaatamisel peaks IS audiitor mõtlema sellele, kas praeguste süsteemidega kaetakse organisatsiooni strateegilised ja toetavad alad. IS audiitor võib läbivaatusesse võtta küsimused selle kohta, kas

- kõik kehtestatud poliitikad koos katavad strateegilised alad, mis on määratletud äritegevuse strateegilise plaanimise protsessiga;

- on olemas protsess, mida tippjuhtkond järgib poliitikale vastavuse detailiseerimiseks, teatavakstegemiseks, nõudmiseks ja seireks;
- on olemas dokumenteeritud poliitikad asjakohaste alade kohta järgnevate hulgast: turvalisus, inimressursid, andmete omandus, lõppkasutaja andmetöötlus, intellektuaalne omand, andmete säilitamine, süsteemide hankimine ja evitamine, väljasttellimine, sõltumatu kinnitus, jätkuvuse plaanimine, kindlustus, privaatsus.
- vaatlusalustes protsessides osalevate inimeste (näiteks andmete omanike, IT juhtkonna, ettevõtte tegevjuhtkonna) rollide ja kohustuste määratlused on nende protsesside toetamiseks sobivad;
- vaatlusalustes protsessides osalevatel inimestel on oma rollide täitmiseks vajalikud oskused, kogemused ja ressursid;
- siseaudit on sobival määral osalenud (kui organisatsioonil on siseauditi ressursse);
- IT-spetsialistide või -talituse koht organisatsioonis on sobiv ja võimaldab organisatsioonil IT kõige paremini ära kasutada oma ärieesmärkide saavutamiseks;
- IT-spetsialistide ja IT-kohustustega mittespetsialistide organisatsioon ja juhtimine on adekvaatne käsitlema vigadest, tegematajätmistest, korratustest või ebaseaduslikest toimingutest tulenevaid riske, mis ähvardavad organisatsiooni.

5 ARUANDLUS

5.1 Aruande koostamine ja järeltoimingud

5.1.1 Auditiaruande kavand tuleks koostada ja läbi arutada koos asjassepuutuva personaliga. Aruandesse tuleb võtta ainult need aspektid, mida toetavad selged asitõendid. Ettepanekud parandusmeetmete kohta tuleks läbi arutada asjakohaste juhtkonda esindavate töötajatega.

5.1.2 Aruanne tuleks viimistleda ISACA suuniste järgi ja esitada juhtkonnale koos soovitustega täiustamise ja probleemide lahendamise ning järeltoimingute kohta.

5.1.3 Tuleks leppida kokku järeltoimingute, tegevuskavade, kohustuste, tähtaegade ning kõrgema juhtkonna määratavate ressursside ja prioriteetide kohta.

6 JÕUSTUMISKUUPÄEV

6.1 See suunis kehtib kõigi infosüsteemiauditite kohta alates 1. maist 2008.

Infosüsteemide auditeerimise protseduurid

Protseduur P1. IS riski kaalutlemine

1 TAUST

1.1 Seos standardite ja suunistega

1.1.1 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.2 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.3 Juhiseid annab suunis G13 "Riski kaalutlemise kasutamine auditi plaanimisel".

1.2 Protseduuri vajadus

1.2.1 See protseduur on kavandatud andma

- IS auditi riski kaalutlemise määratluse;
- juhiseid IS auditi riski kaalutlemise metoodika kasutamise kohta siseauditi talitustes;
- juhiseid riski astmestamise kriteeriumide valimise ja kaalude kasutamise kohta.

2 IS RISK

2.1 Risk on võimalus sellise toimingu või sündmuse toimumiseks, millel on kahjulik toime organisatsioonile ja ta infosüsteemidele. Risk võib olla ka mingi konkreetse ohu potentsiaal mingi vara või varade rühma nõrkuste ärakasutuseks ja seeläbi nende varade kaotsimineku või kahjustuse põhjustamiseks. Harilikult mõõdetakse riski sellise sündmuse toime ja sündmuse asetleidmise sageduse kombinatsiooniga.

2.2 Olemuslikuks riskiks nimetatakse mingi sündmusega seotud riski erimeetmete puudumisel.

2.3 Jääkriskiks nimetatakse mingi sündmusega seotud riski selle sündmuse toimet või tõenäosust vähendavate meetmete olemasolu arvestades.

Protseduur P1. IS riski kaalutlemine (jätkub)

3 IS RISKI KAALUTLEMINE

3.1 Riski kaalutlemine on protsess, mida kasutatakse riskide ja nende võimaliku toime tuvastamiseks ja hindamiseks.

4 IS AUDITI RISKI KAALUTLEMISE METOODIKA

IS auditi riski kaalutlemine on

4.1 IS auditi riski kaalutlemine on metoodika sellise riskimudeli loomiseks, millega optimeerida IS auditi ressursside kinnistamist, organisatsiooni IS-keskkonna ning iga auditeeritava üksusega seotud riskide ammendava tundmaõppimise teel. Auditeeritavaid üksusi käsitleb detailsemalt jaotis 9.

4.2 Riskimudeli eesmärk on optimeerida IS auditi ressursside kinnistamist organisatsiooni IS-kõiksuse ning iga kõiksuseüksusega seotud riskide ammendava tundmaõppimise teel.

5 RISKIPÕHINE LÄHENEMINE IS AUDITILE

5.1 Üha suurem arv organisatsioone siirdub riskipõhisele auditikäsitlusele, mida saab rakendada pideva auditiprotsessi väljatöötamiseks ja täiustamiseks. Seda lähenemisviisi kasutatakse riski kaalutlemiseks ning IS audiitori abistamiseks vastavuskontrolli või sõltumatu kontrolli tegemise otsustamisel. Riskipõhise auditikäsitluse puhul toetuvad IS audiitorid mitte ainult riskile. Nad toetuvad ka sise- ja käitusmeetmetele ning organisatsiooni tundmisele. Sedalaadi riski kaalutlemise otsus võib aidata siduda juhtimise tasuvusanalüüsi tuntud riskiga ja võimaldada praktilisi valikuid.

5.2 Äritegevuse iseloomu tundma õppides saavad IS audiitorid tuvastada ja liigitada riskitüüpe, mis paremini määravad läbivaatuse sooritamiseks kasutatava riskimudeli või lähenemise riskidele. Riski kaalutlemise mudeliks võib olla lihtsalt riski määramise avaldis, milles äritegevusega seotud riskitüüpidele luuakse kaalud. Teisalt võib riski kaalutlemine olla skeem, milles riskidele on antud keerukamad kaalud, mis põhinevad äritegevuse iseloomul või riski olulisusel.

5.3 IS audiitorit huvitavad ohjamata riskid ja elutähtsad meetmed. Riskipõhise auditile lähenemise puhul huvitavad IS audiitorit seetõttu tehnoloogiapõhised süsteemid, mis pakuvad juhtimismehhanisme suure olemusliku riskiga ärifunktsioonidele, ja aktsepteeritavast suurema jääkriskiga tehnoloogiapõhised funktsioonid.

5.4 Riskide astmestuse esimene eeltingimus on IS auditi kõiksuse määratlemine. Auditi kõiksuse määramine põhineb organisatsiooni IT strateegilise plaani ja organisatsiooni tegutsemise tundmisel, organisatsiooniskeemide ja kõigi organisatsiooni liikmete funktsiooni ja kohustuste määrangute läbivaatusel ning vestlustel vastutavate juhtkonna liikmetega.

5.5 Harilikult viiakse auditi plaanimistsüklid kooskõlla äritegevuse plaanimistsüklitega. Sageli valitakse aastane auditi plaanimistsükkel – kalendriaasta või muu kaheteistkuune periood. Mõnedel organisatsioonidel on kaheteistkuuste perioodide asemel näiteks kuue- või kaheksateistkuune. Püsiva plaanimistsükli asemel kasutavad mõned organisatsioonid libisevaid plaanimistsükleid, mis libisevad edasi mingi seatava perioodi võrra. Järjekindluse saavutamiseks eeldab käesolev protseduur aastast plaanimistsüklit.

5.6 Auditiprojektide valimine IS auditite plaani lülitamiseks on üks kõige tähtsamaid IS auditi juhtkonna ees seisvaid probleeme. Auditite plaanimise protsess annab võimaluse kvantiteerida ja põhjendada IS auditeerimise aastaplaani täitmiseks vajalike IS auditi ressursside kogust. Kui ei õnnestu valida sobivaid projekte, jäävad ära kasutamata võimalused tõsta juhtimise ja tegutsemise toimivust.

5.7 IS auditiplaani aluseks on eeldus, et tulevaste auditiläbivaatuste või -projektide hindamine on toimivam, kui läbivaatuste või projektide valimise otsuste tegemiseks vajaliku teabe kogumisel järgitakse mingit formaalset protsessi. Siinkirjeldatavad lähenemisviisid kujutavad endast põhiliselt raamstruktuuri, milles rakendada tervet mõistust ja kutsealast otsustusvõimet.

5.8 Esitatud metoodika on suhteliselt lihtne. Valdaval enamikul juhtudel peaks temast aga piisama IS auditiläbivaatuste või -projektide valimise mõistlike, kainete ja õigustatavate otsusteni jõudmiseks. Selles protseduuris on detailiseeritud üks raamstruktuur, mida kasutada riskile avatuse analüüsi sooritamisel ning auditiläbivaatuste või -projektide prioriteetide järjestamisel.

5.9 Siin kasutatakse riski kaalutlemist sellise meetodi tähenduses, mida kasutatakse auditeeritavate üksuste uurimiseks ning riskile kõige enam avatutega seotud läbivaatuste või projektide valimiseks. Riski kaalutlemisega lähenemine auditiläbivaatuse või -projekti valimisele on tähtis selle poolest, et ta pakub vahendeid mõistliku kinnituse saamiseks sellele, et IS auditi ressursid jaotatakse optimaalselt, st IS auditite plaan jaotab IS auditi ressursid nii, et see annab tõenäoliselt maksimaalselt kasu. Selleks annab riski kaalutlemisega lähenemine otsesed kriteeriumid, mille järgi süstemaatiliselt valida auditiprojekte. Plaanilise IS auditi täieliku katvuse detailiseerimiseks seotakse IS auditite plaan sageli rahandusliku ja käitusliku auditiplaaniga.

6 IS RISKI KAALUTLEMISE MENETLUSED

6.1 Kui IS audiitoril tuleb otsustada, milliseid tegevusliine tuleks auditeerida, võib ta ees olla suur valik auditeerimisobjekte. Võimaluse korral tuleks riski kaalutlemisse lülitada kõik organisatsiooni IS-alad. Mõned organisatsioonid hindavad ainult

Protseduur P1. IS riski kaalutlemine (jätkub)

IS-projekte, teised aga iga auditeeritavat IS ala või süsteemi. Mõlemal juhul võib esineda mitmesugust tüüpi auditiriske. IS audiitor peaks hindama neid mitmesuguseid riskikandidaate, et teha kindlaks, millistel aladel on risk suur ja mida tuleb seetõttu auditeerida. Selle protsessi eesmärk on

- tuvastada alad, kus jääkrisk on vastuvõtmatult suur;
- tuvastada elutähtsad juhtimissüsteemid, mis käsitlevad suuri olemuslikke riske;
- hinnata elutähtsate juhtimissüsteemide puhul eksisteerivat määramatust.

6.2 Riski kaalutlemise kasutamine auditeerimisele kuuluvate IS-alade määramiseks

- võimaldab juhtkonnal toimivalt jaotada piiratud IS auditi ressursse;
- annab mõistliku kinnituse sellele, et juhtkonna kõigilt tasemetelt, sealhulgas juhatuselt ja tegevusliini juhtkonnalt on hangitud asjakohane teave. Üldiselt sisaldab see teave niisugust, mis aitab juhtkonnal toimivalt täita oma kohustusi ja annab mõistliku kinnituse sellele, et IS auditi tegevused on suunatud suure äririskiga aladele, ning pakub juhtkonnale väärtust;
- loob aluse IS auditi talituse toimivale haldusele;
- teeb kokkuvõtte sellest, kuidas läbivaatuse üksikobjekt on seotud kogu organisatsiooniga ja äriplaanidega.

7 IS RISKI KAALUTLEMISE MEETODID

7.1 IS riski kaalutlemiseks on praegu kasutusel mitu meetodit. Üks selliseid IS auditite prioriteetimiseks kasulikke meetodeid on riskitegurite hindamisel põhinev punktisüsteem, mis arvestab selliseid muutujaid nagu tehniline keerukus, süsteemide ja protsesside muutumise ulatus ja kaalukus. Need muutujad võivad olla kaalutud või mitte. Seejärel võrreldakse neid riskide väärtusi omavahel ja harilikult koostatakse IS auditeerimise aastaplaan. Sageli kinnitab auditiplaani auditikomisjon või tegevjuhataja. Seejärel ajastatakse läbivaatused vastavalt auditiplaanile. Üks riski kaalutlemise vorme on takseeriv; see kujutab endast sõltumatu otsuse tegemist tegevjuhtkonna suuniste, ajaloovaadete ja tegutsemiskliima põhjal.

8 ANDMETE KOGUMINE

8.1 Organisatsiooni tegutsemise kõiki aspekte kirjeldavat teavet kasutatakse mitmesuguste auditeeritavate üksuste määratlemiseks ja üksuse tegutsemisele omaste IS-riskide modelleerimiseks. Niisuguste andmete allikate hulka kuuluvad

- vestlused kõrgema juhtkonnaga, eesmärgiga koguda andmeid IS-riskimudeli koostamiseks;
- juhtkonnale IS-riskimudeli andmete kogumise hõlbustamiseks saadetud struktureeritud küsimustiku vastused;

- eelmised läbivaatuste aruanded;
- IT strateegiline plaan;
- eelarvestuse protsess, mis võib olla kasulik teabeallikas;
- välisaudiitorite tõstatatud küsimused;
- oluliste küsimuste kohta kõigist muudest allikatest kogutud IS auditi teadmus ja teadlikkus;
- andmete kogumise spetsiifilised meetodid, kui nad on piisavad, arvestades töö tegemiseks kasutada olevat aega ja ressursse.

9 IS AUDITEERITAVAD ÜKSUSED

9.1 Eelnimetatud mudel on mõeldud sisaldama ja looma riskihinnet organisatsiooni (IS auditeerimise kõiksuse) IS iga auditeeritava üksuse kohta. Auditeeritavat üksust võib määratleda kui iga organisatsiooni ja ta süsteemide diskreetset lõiku. Mingi konkreetse auditeeritava üksuse määramiseks või eristamiseks ei ole kindlaid reegleid, kuid selles auditi riskimudelis võib iga üksuse, teema või funktsiooni puhul kasutada järgmisi juhiseid:

- on auditeeritav mõistliku ajaga;
- on süsteem, st tal on tuvastatavad sisendid, protsessid, väljundid ja tulemid;
- on eraldatav, st teda saab auditeerida minimaalse teistele süsteemidele toetumisega. (See võib olla raske, kui läbivaadatava rakendussüsteemiga on liidestatud palju süsteeme.)

10 NÄITEID

10.1 IS riski kaalutlemiseks on palju mitmesuguseid meetodeid. Mitut kaalutlemise tüüpi on kirjeldatud jaotistes 11, 12, 13 ja 14.

11 NÄIDE I

11.1 Näide I demonstreerib riski kaalutlemist kaheksa keskse muutujaga. IS auditi kõiksuse igale üksusele või alale antakse hinne nende kaheksa keskse muutuja järgi, kasutades kirjeldavaid arvväärtusi ühest (väike) viieni (suur). Nende hindamisotsuste tulemid korrutatakse seejärel olulisuse kaaluteguritega, mille skaala ulatub ühest (väike) kümneni (suur) ja saadakse laiendatud väärtused. Näitesse I on võetud olulisuse kaalutegurite suvalised näited. Koguväärtuse saamiseks liidetakse saadud laiendatud väärtused. Kui iga auditeeritava üksuse või ala kohta on saadud niisugused koguväärtused, astmestatakse auditeeritavad üksused või alad riski järgi. Seejärel koostatakse nende astmete põhjal IS auditi aastaplaani raamstruktuur. Nimetatud kaheksa keskset muutujat on koos lühiseletustega loetletud jaotistes 11.1.1, 11.1.2 ja 11.1.3.

Protseduur P1. IS riski kaalutlemine (jätkub)

11.1.1 Toime mõõdud

- Tegevuse iseloom: tegevuse ja seda tegevust kasutava organisatsiooniosa elutähtsus. Harvad või ebatavalised tegevused või projektid tekitavad tõenäolisemalt vigu või ebatõhusust ning pakuvad auditile suuremat huvi.
- Taandumise korraldus: see tegur puudutab meetmeid, mis on kasutusel töö jätkamiseks uue süsteemi probleemide puhul. Arvestada tuleks jätkusuutlikkuse plaane, käsiprotseduure ja vana süsteemi.

Üldiselt on nii, et kui ülalloetletuga on tegeldud, kui see on teostatav või tasuv, on risk kõige väiksem.

- Selle tegevusliini tundlikkus täitevjuhtkonnale. See tegur näitab, kui tähtsaks peab tegevjuhtkond seda üksust, tegevusliini või ala.
- Kaalukus: see mõiste puudutab mingi teabeüksuse tähtsust ta toime järgi organisatsiooni talitlusele. Väljendab mingi üksikküsimuse suhtelist olulisust või tähtsust kogu organisatsiooni kontekstis.

11.1.2 Tõenäosuse mõõdud

- Süsteemi või protsessi muutumise ulatus: dünaamiline keskkond süsteemi või protsessi muutumise mõttes suurendab vigade tõenäosust ja seega suurendab auditi huvi. Võib leida aset ulatuslik protsessi ümberrajamine. Süsteemi või protsessi muudatus toimub harilikult täiustuse saavutamiseks pikema aja pärast, kuid sageli on tal lühiajalised kõrvaltoimed, mis nõuavad auditi suuremat katvust.
- Keerukus: see riskitegur kajastab vigade või vääromastamise avastamata jäämise tõenäosust keeruka keskkonna tõttu. Keerukuse hinne sõltub paljudest teguritest. Otsuseid keerukuse kohta konkreetses auditis mõjutavad automatiseerituse ulatus, arvutuste keerukus, tegevuste vastastikune seotus ja vastastikune sõltuvus, toodete või teenuste arv, hinnangute ajastused, sõltuvus kolmandatest pooltest, kliendi nõuded, töötlusajad, kohaldatavad õigusaktid ja paljud muud tegurid, osa neist tundmatud.
- Projektihaldus. Projektihalduse astmestamisel tuleks võtta arvesse järgnev:

  - oma või välised väljatöötajad,
  - projekti struktuur,
  - personali oskused,
  - projekti tähtajad.

Üldiselt on projekti väljasttellimise korral risk jaotatud.

11.1.3 Meetmete määramatuse mõõdud

- Eelmisest läbivaatusest möödunud aeg. Eelmisest läbivaatusest möödunud aja pikenemisel uue läbivaatuse väärtus tõenäoliselt kasvab. Läbivaatuse kasulik toime on kõige suurem vahetult enne või pärast süsteemi teostamist.

Protseduur P1. IS riski kaalutlemine (jätkub)

Näide I. IS riski kaalutlemine

KESKSED MUUTUJAD	**KIRJELDAV VÄÄRTUS** 1 (väike) kuni 5 (suur)	**OLULISUSE KAAL** 1 (väike) kuni 10 (suur)	**LAIENDATUD VÄÄRTUS**
1. Tegevuse iseloom	**Arvesse võtta:** tuumtegevus = 4 kuni 5 tuluüksus = 2 kuni 3 lokaalne süsteem = 1	8*	
2. Taandumine	**Arvesse võtta:** jätkusuutlikkuse plaanid avariijärgse taaste plaanid käsiprotseduurid vana süsteem	5*	
3. Tegevusliini tundlikkus täitevjuhtkonnale	Suur huvi = 4 kuni 5 Mõõdukas huvi = 2 kuni 3 Väike huvi = 1	6*	
4. Kaalukus	**Loodava tulu või tarbitavate ressursside olulisus:** projekti eelarve >$500000 = 4 kuni 5 projekti eelarve $100000...500000 = 2 kuni 3 projekti eelarve <$100000 = 1 tulu/kulu >$500000 = 4 kuni 5 tulu/kulu $100000...500000 = 2 kuni 3 tulu/kulu <$100000 = 1	5*	
5. Süsteemi, protseduuri, protsessi muutuse ulatus	**Arvesse võtta:** ümberrajamise ulatus; suur ümberrajamine = 4 kuni 5 mõõdukas ümberrajamine = 2 kuni 3 väike ümberrajamine = 1 või protseduure pole = 4 või 5 lokaalsed protseduurid = 3 või 2 üleorganisatsioonilised protseduurid = 1	8*	
6. Keerukus	**Arvesse võtta:** tehingute maht kasutajate arv tsentraliseeritud või detsentraliseeritud liideste arv väga keeruline = 4 kuni 5 mõõdukalt keeruline = 2 kuni 3 lihtne = 1	7*	
7. Projektihaldus	**Arvesse võtta:** oma või välised väljatöötajad projekti struktuur personali oskused projekti tähtajad	7*	
8. Eelmisest läbivaatusest möödunud aeg	Hinne 5: eelmisest auditist on möödunud vähemalt 5 aastat või auditit pole varem olnud	1*	
	Kokku		

* On kasutatud suvalisi näitelisi kaalutegureid.

Protseduur P1. IS riski kaalutlemine (jätkub)

12 NÄIDE II

12.1 Näide II laiendab näites I kasutatud IS-riski kaalutlemist, hõlmates äririske ja ka näites I kasutatud kaheksat IS auditi keskset muutujat. IS auditi riski kaalutegur näitest I korrutatakse näites II äririskiga. Äririskitegureid (rahalist, strateegilist, tegutsemisalast ja õiguslikku) arvestatakse nende relevantsuse järgi iga auditeeritava üksuse või ala puhul.

12.2 Iga IS auditi kõiksuse üksus või ala puhul hinnatakse neid kaheksat keskset muutujat arvväärtusega 1 (väike) kuni 5 (suur). Nende hindamisotsustuste tulemid korrutatakse olulisuse kaaluteguriga vahemikust 1 (väike) kuni 10 (suur), nagu näites I. Niisugused laiendatud väärtused liidetakse koguhinde saamiseks (kasutades meelevaldseid kaalutegureid näitest I). Saadud koguhinne on IS auditi riski astmestustegur.

12.3 Alljärgnevas on määratletud ülalnimetatud neli äririskitegurit.

- Rahaline risk. Kuna enamikul süsteemidest on potentsiaalselt mingi toime organisatsiooni rahalistele tulemustele, tuleks arvestada selliste mõjude suurust ja tõenäosust. Kui oodatav toime on kaudne ja suhteliselt väike võrreldes süsteemi muude toimete ja otstarvetega ja/või võrreldes muude auditeeritavate alade või süsteemide omaga, tuleks rahalise riskiteguri hindeks tõenäoliselt panna mitte 1, vaid 0.
- Strateegiline risk. Süsteemidel võib olla organisatsioonidele otsene strateegiline toime. Mõned sellised toimed, mille tõttu riskiteguri väärtus võiks olla 1, on tuvastanud täitevjuhtkond.
- Tegutsemisrisk. Tegutsemisriskile antakse väärtuseks 1 tõenäoliselt sagedamini kui ükskõik millisele teisele äririskitegurile, sest enamik süsteeme on kavandatud mõjutama seda, kuidas ja kui toimivalt organisatsioon sooritab oma igapäevast äritegevust.
- Õiguslik risk. Süsteemid võivad otseselt mõjutada seda, kuidas organisatsioon järgib õigusnorme.

12.4 Igale äririskitegurile kinnistatakse relevantsustegur väärtusega 1 (relevantne) või 0 (pole relevantne). Seejärel korrutatakse iga relevantsustegur talle vastava kaaluga ja liidetakse korrutised selle auditeeritava ala summaarse äririskiteguri saamiseks.

12.5 Relevantsustegurite kinnistamisel tuleks arvestada järgmist kolme aspekti.

- Millised on auditeeritava süsteemi eeldatavad otstarbed ja eesmärgid?
- Milline on auditi eeldatav käsitlusala ja eesmärgistik?
- Kas süsteem mõjutab otseselt organisatsiooni rahalist, strateegilist, tegevusalast või õiguslikku sooritust? Kui näiteks süsteem ei tööta nii, nagu on mõeldud, kas on võimalik, et organisatsioon kannab rahalist kahju, kogeb strateegilist tagasilööki, tal on tegutsemisprobleeme või ta on vastuolus õigusnormidega?

12.6 Viimane samm selles näites on auditiriski hinde korrutamine äririskiteguriga riski koondhinde saamiseks. Vt näide alljärgnevas tabelis. Kui iga auditeeritava üksuse või ala kohta on saadud riski koondhinne, astmestatakse auditeeritavad üksused või alad riski järgi. Seejärel koostatakse nende astmete põhjal IS auditi aastaplaani raamstruktuur.

Näide II. IS riski kaalutlemine äririskitegureid arvestades

AUDITEERITAV ÜKSUS	AUDITIRISKI HINNE (Näitest I)	ÄRIRISKITEGURID (VÄÄRTUS 0 VÕI 1)				ÄRIRISKITEGUR	RISKI KOONDHINNE
		RAHALINE	STRATEEGILINE	TEGEVUSALANE	ÕIGUSLIK		
Äritegevus	**Riski kaal**	**5***	**4***	**3***	**2***		
Rahandussüsteem	158	1	1	1	0	12	1896
Jätkusuutlikkus	162	0	0	1	1	5	810
Palgafond	165	0	0	1	0	3	495
Kohtvõrgud	159	0	0	1	0	3	477
Arvutikäitus	146	0	0	1	0	3	438
Tarkvaralitsentsid	123	0	0	0	1	2	246
Ressursipääsu reguleerimine	152	0	0	1	0	3	456

Näiteks rahandussüsteem: 158*(5*1+4*1+3*1+2*0) = 158*(5+4+3) = 158*12 = 1896

13 NÄIDE III

13.1 Mõned IS audiitorid eelistavad reastada ainult IS-projekte, mitte aga kogu IS auditeeritavat kõiksust. Näide III pakub üht metoodikat IS-projektide reastamiseks. IS auditeerimise kõiksuses hinnatakse iga projekti eelnimetatud kaheksa keskse muutuja põhjal, kasutades riski hindeks arvväärtusi 1 (väike) kuni 5 (suur). Laiendatud väärtuse saamiseks korrutatakse need hindamisotsused seejärel kaaluteguriga, mille väärtus võib olla 1 (väike) kuni 10 (suur). Summaarse väärtuse saamiseks liidetakse need laiendatud väärtused. Kui on saadud iga projekti summaarsed väärtused, hinnatakse projektid riski järgi. Nendest hinnetest tuletatakse seejärel iga-aastase IS auditeerimise projektikatvuse raamstruktuur. Näites III kasutatud kategooriad on loetletud jaotistes 13.2 ja 13.3.

13.2 Toime mõõdud

- Projekti eelarve. Tähtis tegur, mida arvestada, on IS projekti koondeelarve. Juhinduda võib sellest, et mõned organisatsioonid võtavad US$500000 ületavate projektieelarvete puhul riski väärtuseks 4 või 5. Need organisatsioonid võtavad US$100000 kuni US$500000 suuruste eelarvete puhul riski väärtuseks 2 või 3 ja kuni US$100000 suuruste eelarvete puhul võtavad väärtuseks 1.
- Tehingute maht. Vaatlusaluses süsteemis mingil etteantud perioodil töötlemisele kuuluvate tehingute hinnanguline kogumaht.

Protseduur P1. IS riski kaalutlemine (jätkub)

- Tegevuse iseloom. Tegevuse ja seda tegevust kasutava organisatsiooniosa elutähtsus. Harvad või ebatavalised tegevused või projektid tekitavad tõenäolisemalt vigu või ebatõhusust ning pakuvad auditile suuremat huvi.
- Tegevjuhtkonna huvi. See tegur näitab, kui tähtsaks peab tegevjuhtkond seda üksust, tegevusliini või ala.
- Taandumise korraldus. See tegur puudutab meetmeid, mis on kasutusel töö jätkamiseks uue süsteemi probleemide puhul. Arvesse tuleks võtta järgmised tegurid:
  - jätkusuutlikkuse plaanid,
  - avariijärgse taaste plaanid,
  - käsiprotseduurid,
  - vana süsteem.

Üldiselt on nii, et kui ülalloetletuga on tegeldud, kui see on teostatav või tasuv, on risk kõige väiksem.

13.3 Tõenäosuse mõõdud

- Protseduuride muudatused. Süsteemi teostamisega kaasneva protseduuride muutmise või ümberrajamise ulatus.
- Süsteemi keerukus. Tuleks arvestada selliseid tegureid nagu kasutajate arv, süsteemi moodulite arv, suurarvuti või klient-server-keskkond (tsentraliseeritud või detsentraliseeritud keskkond) ja liideste arv.
- Projektihaldus. Projektihalduse astmestamisel tuleks võtta arvesse järgnev:
  - oma või välised väljatöötajad,
  - projekti struktuur,
  - personali oskused,
  - projekti tähtajad.

Üldiselt on projekti väljasttellimise korral risk jaotatud.

Näide III. IT-projekti riski astmestamine

Kategooria	Riski väärtus 1 (väike) kuni 5 (suur)	Olulisuse kaal 1 (väike) kuni 10 (suur)	Kaalutud väärtus
1. Projekti eelarve >$500000 = 4 kuni 5 $100000 kuni 500000 = 2 kuni 3 <$100000 = 1		5	
2. Tehingute maht		2	
3. Tegevuse iseloom Tuumjuhatus 4 kuni 5 Tuluüksus 2 kuni 3 Lokaalne süsteem 1		8	
4. Tegevjuhtkonna huvi Suur huvi = 4 kuni 5 Mõõdukas huvi = 2 kuni 3 Väike huvi = 1		6	
5. Taandumise korraldus Jätkusuutlikkuse ja avariijärgse taaste plaanid Käsiprotseduurid Vana süsteem		7	
6. Protseduuride muudatused (ümberrajamise ulatus) Suur ümberrajamine = 4 kuni 5 Mõõdukas ümberrajamine = 2 kuni 3 Väike ümberrajamine = 1		8	
7. Süsteemi keerukus Kasutajate arv Moodulite arv Tsentraliseeritud või detsentraliseeritud (suurarvuti või klient-server) Liidesed		7	
8. Projektihaldus Oma väljatöötus Välised väljatöötajad Struktuur Oskused Tähtajad		7	
		Kokku	

14 NÄIDE IV. AUDITEERITAVATE ÜKSUSTE IS RISKI KAALUTLEMINE

14.1 Näide IV astmestab IS auditeeritava kõiksuse mitmesugused auditeeritavate üksuste kategooriad, kui need on piiritletud. Kategooriad loetletakse neid üksusi ähvardava riski iseloomu põhjal. Kogutakse asjassepuutuv teave, näiteks rahalise ohtudele avatuse, äritoime ja käsitlusala kohta. Kategooriad on järgmised:

i. arvutuskeskuse käitus,
ii. rakendussüsteemid (tööks),
iii. rakendussüsteemid (arenduseks);
iv. IS hankimine (tööjõud ja materjalid),
v. tarkvarapakettide hankimine,
vi. muud IS funktsioonid.

14.2 Iga kategooria all on loetletud peamised riskielemendid. Sõltuvalt riski tüübist on igale riskielemendile kinnistatud kaal. Iga riskielementi on seejärel detailiseeritud, lisades talle lähtehinde astmiku. Igale riskielemendile antav kaalutud hinne on lähtehinde ja ta kaalu korrutis. Funktsiooni koondhinne on kõigi ta riskielementide kaalutud hinnete summa. Võrdluse hõlbustamiseks mõõdetakse kaalutud hindeid 100-pallisel skaalal[3]. Iga auditeeritava üksuse kohta võib koostada eraldi riskikaalutluslehed. Lõpuks tehakse kokkuvõte kõigi auditeeritavate üksuste koondhinnetest ja määratakse auditite prioriteedid.

Näide IV. Riski kaalutlemine. IS audit. 1. Arvutuskeskuse käitus

	Astmik	Kaal	Hinne	Kaalutud hinne
1	**Arvutuskeskuse töötajate arv**	1		5
	Väga väike (alla 2)		1	
	Väike (3 kuni 7)		2	
	Keskmine (7 kuni 15)		3	
	Suur (16 kuni 25)		4	
	Väga suur (üle 25)		5	
2	**Toime grupi äritegevusele**	5		25
	Puudub		1	
	Väike		2	
	Mõõdukas		3	
	Suur		4	
	Lõpetab grupi äritegevuse		5	
3	**Rakenduste arv**	5		25
	Üksainus		1	
	Alla 5		2	
	5 kuni 15		3	
	16 kuni 25		4	
	Üle 25		5	
4	**Kasutajate arv**	2		10
	Alla 25		1	
	26 kuni 50		2	
	51 kuni 100		3	
	100 kuni 250		4	
	Üle 250		5	
5	**Eelmiste auditite leiud**	1		5
	Olulisi leide polnud		1	
	Mõned ebaolulised leiud		2	
	Palju ebaolulisi leide		3	
	Mõned olulised leiud		4	
	Palju olulisi leide		5	
6	**Töötluse keerukus**	2		10
	Pakktöötlus		1	
	Pakk- ja reaalajatöötlus		2	
	Pakk-, reaalaja- ja sidustöötlus		3	
	Klient-server-töötlus		4	
	Rööp- või hajustöötlus		5	

[3] Näide tabelites illustreerib seda sobiv kaalude valimine ja maksimaalse lähtehinde andmine igale riskielemendile, nii et koondhindeks saadakse 100, mis on seega skaala maksimum. Tõlkija m.

Protseduur P1. IS riski kaalutlemine (jätkub)

7	**Seadmete, platvormi, personali muutused**	1		5
	Muutusteta		1	
	Mõõdukad muutused, vähene vahetumine		2	
	Platvormi muutused, vähene vahetumine		3	
	Suur vahetumine		4	
	Platvormi muutused ja suur vahetumine		5	
8	**Platvormide arv**	3		15
	1		1	
	2		2	
	3		3	
	4		4	
	5 või rohkem		5	
	Riski koondhinne			100

Näide IV. Riski kaalutlemine. IS audit. 2. Rakendussüsteemid (tootmiseks)

	Astmik	**Kaal**	**Hinne**	**Kaalutud hinne**
1	**Süsteemi tõrke toime (elutähtsus)**	5		25
	Vahetu toime puudub		1	
	Ebamugavus kasutajatele		2	
	Maine kaotus		3	
	Tulu kaotus		4	
	Äritegevuse, tulu ja maine kaotus		5	
2	**Rahaline avatus riskile (AED)**	5		25
	Puudub		1	
	Väike (alla 100000)		2	
	Mõõdukas (100000 kuni 1 mln)		3	
	Suur (1 mln kuni 10 mln)		4	
	Väga suur (üle 10 mln)		5	
3	**Süsteemi käsitlusala**	2		10
	Osakonna osa		1	
	Kogu osakond		2	
	Mitu osakonda		3	
	Kogu organisatsioon		4	
	Organisatsioon ja väljaspool		5	
4	**Rakenduse iga**	1		5
	Üle 10 a		1	
	7 kuni 10 a		2	
	4 kuni 6 a		3	
	1 kuni 3 a		4	
	Alla aasta		5	
5	**Eelmiste auditite leiud**	2		10
	Hiljutine audit: nõrkusi polnud		1	
	Hiljutine audit: oli väikesi nõrkusi		2	
	Audit: mõned nõrkused		3	
	Audit: palju nõrkusi		4	
	Pole varem auditeeritud		5	
6	**Rakenduse suurus (programmide arv)**	3		15
	Alla 25		1	
	26 kuni 50		2	
	50 kuni 100		3	
	100 kuni 250		4	
	Üle 250		5	
7	**Keskkonna või personali muutused**	1		5
	Muutusteta		1	
	Mõõdukad muutused, vähene vahetumine		2	
	Olulised muutused, vähene vahetumine		3	
	Suur vahetumine		4	
	Olulised muutused ja suur vahetumine		5	
8	**Evituse asukohtade arv**	1		5
	1		1	
	2		2	
	3		3	
	4		4	
	5 või rohkem		5	
	Riski koondhinne			100

Protseduur P1. IS riski kaalutlemine (jätkub)

Näide IV. Riski kaalutlemine. IS audit. 3. Rakendussüsteemid (arendustööks)

	Astmik	Kaal	Hinne	Kaalutud hinne
1	**Meeskonna suurus, korraldus ja kogemus**	3		15
	Väike, spetsialiseeritud ja kogenud meeskond		1	
	Keskmise suurusega, tsentraliseeritud ja kogenud meeskond		2	
	Keskmine, kogenud, segaprioriteetidega		3	
	Keskmine, peamiselt tsentraliseeritud, muude prioriteetidega		4	
	Suur, detsentraliseeritud, kogemusteta, ebaselge alluvusliin		5	
2	**Süsteemi suurus**	3		15
	Väike arv programme, ühele osakonnale		1	
	Keskmine arv programme, ühele osakonnale		2	
	Palju programme, paljudele osakondadele		3	
	Keskmine arv programme, kogu organisatsioonile		4	
	Palju programme, kogu organisatsioonile		5	
3	**Arendustsükli kestus**	2		10
	Alla 3 kuu		1	
	3 kuni 6 kuud		2	
	6 kuni 12 kuud		3	
	1 kuni 1,5 a		4	
	2 aastat või kauem		5	
4	**Arendusplatvorm**	3		15
	Läbiproovitud ja laialt kasutusel		1	
	Üsna uus, kuid ülemaailmselt tunnustatud		2	
	Üsna uus, kuid ülemaailmse tunnustuseta		3	
	Äraproovitud ja valmistajaspetsiifiline		4	
	Uus, proovimata, valmistajaspetsiifiline		5	
5	**Eelmiste auditite gõlmatus**	2		10
	Meetmete loomise proov		1	
	Nõuete analüüsi järk		2	
	Projekti ajakava seire		3	
	Projekti kulude seire		4	
	Puudub		5	
6	**Süsteemiarenduse metoodika**	3		15
	Tüüpmetoodika, dokumenteeritud standardite ja protseduuridega		1	
	Tüüpmetoodika, dokumenteeritud standardite ja protseduurideta		2	
	Tüüpmetoodikata, kuid kogenud meeskond		3	
	Katseline läbiproovimata metoodika		4	
	Arendusmetoodikata, dokumenteeritud arendusstandardite ja -suunisteta		5	
7	**Projektihalduse kogemus**	1		5
	Väga suur		1	
	Üle keskmise		2	
	Keskmine		3	
	Alla keskmise		4	
	Kogemused puuduvad või mitu projekti korraga		5	
8	**Välise tööjõu kasutamine**	1		5
	Väike arv, üksainus tarnija		1	
	Väike arv, eri tarnijad		2	
	Tunduv arv, üksainus tarnija		3	
	Tunduv arv, eri tarnijad		4	
	100%		5	
	Riski koondhinne			100

Näide IV. Riski kaalutlemine. IS audit. 4. IS hankimine (tööjõud ja materjal)

	Astmik	Kaal	Hinne	Kaalutud hinne
1	**Toime**	5		25
	Vahetu toime puudub		1	
	Ebamugavus kasutajatele		2	
	Maine kaotus		3	
	Tulu kaotus		4	
	Äritegevuse, tulu ja maine kaotus		5	
2	**Rahaline avatus riskile (AED)**	5		25
	Puudub		1	
	Väike (alla 100000)		2	
	Mõõdukas (100000 kuni 1 mln)		3	
	Suur (1 mln kuni 10 mln)		4	
	Väga suur (üle 10 mln)		5	

Protseduur P1. IS riski kaalutlemine (jätkub)

3	**Protseduurid ja suunised**	5		25
	Dokumenteeritud ja testitud protseduurid		1	
	Dokumenteerimata protseduurid		2	
	Protseduurid on, kuid pole täielikult evitatud		3	
	Protseduure pole kehtestatud, kuid reguleeritakse		4	
	Protseduure pole kehtestatud, ei reguleerita		5	
4	**Eelmiste auditite leiud**	2		10
	Hiljutine audit: nõrkusi polnud		1	
	Hiljutine audit: oli väikesi nõrkusi		2	
	Audit: mõned nõrkused		3	
	Audit: palju nõrkusi		4	
	Pole varem auditeeritud		5	
5	**Keerukus**	3		15
	Kohalikud allikad, ühele osakonnale		1	
	Kohalikud allikad, kogu organisatsioonile		2	
	Rahvusvahelised allikad, üks tehnoloogia		3	
	Rahvusvahelised allikad, mitu tehnoloogiat		4	
	Rahvusvahelised ja kohalikud allikad, mitu tehnoloogiat		5	
	Riski koondhinne			100

Näide IV. Riski kaalutlemine. IS audit. 5. Tarkvarapakettide hankimine

	Astmik	**Kaal**	**Hinne**	**Kaalutud hinne**
1	**Süsteemi käsitlusala**	5		25
	Osakonna osa		1	
	Kogu osakond		2	
	Mitu osakonda		3	
	Kogu organisatsioon		4	
	Organisatsioon ja väljaspool		5	
2	**Rahaline avatus riskile (AED)**	5		25
	Puudub		1	
	Väike (alla 100000)		2	
	Mõõdukas (100000 kuni 1 mln)		3	
	Suur (1 mln kuni 10 mln)		4	
	Väga suur (üle 10 mln)		5	
3	**Paketi iseloom**	2		10
	Sarjatoode		1	
	Tellimustöö tarnijalt, hooldab tarnija		2	
	Tarnija väljatööde, hooldus sisemine		3	
	Ühisväljatööde, hooldab tarnija		4	
	Ühisväljatööde, hooldus sisemine		5	
4	**Hindaja**	1		5
	Kasutav osakond, IS, konsultant		1	
	IS, kasutaja		2	
	Konsultant		3	
	IS		4	
	Kasutav osakond		5	
5	**Paketi maksumus ja keerukus**	2		10
	Tühine		1	
	Väike		2	
	Mõõdukas		3	
	Suur		4	
	Väga suur		5	
6	**Hindamismetoodika**	3		15
	Hinnatakse tarnijat ja toodet		1	
	Hinnatakse ainult toodet		2	
	Hinnatakse ainult tarnijat		3	
	Ei hinnata, hangitakse tingimustega		4	
	Ei hinnata, hangitakse tingimusteta		5	
7	**Valimine**	1		5
	Valitakse paljude kandidaatide hulgast		1	
	Valitakse väheste, mainekate tarnijate hulgast		2	
	Valitakse väheste, tuntud süsteemide hulgast		3	
	Valitakse mingi tuttav süsteem		4	
	Valitakse mingi tundmatu süsteem		5	

Protseduur P1. IS riski kaalutlemine (jätkub)

8	**Toime äritegevusele**	1		5
	Vahetu toime puudub		1	
	Ebamugavus kasutajatele		2	
	Maine kaotus		3	
	Tulu kaotus		4	
	Äritegevuse, tulu ja maine kaotus		5	
	Riski koondhinne			100

Näide IV. Riski kaalutlemine. IS audit. 6. Muud IS funktsioonid

	Astmik	**Kaal**	**Hinne**	**Kaalutud hinne**
1	**Funktsiooni tõrke toime (elutähtsus)**	5		25
	Vahetu toime puudub		1	
	Ebamugavus kasutajatele		2	
	Maine kaotus		3	
	Tulu kaotus		4	
	Äritegevuse, tulu ja maine kaotus		5	
2	**Rahaline avatus riskile (AED)**	5		25
	Puudub		1	
	Väike (alla 100000)		2	
	Mõõdukas (100000 kuni 1 mln)		3	
	Suur (1 mln kuni 10 mln)		4	
	Väga suur (üle 10 mln)		5	
3	**Funktsiooni käsitlusala**	2		10
	Osakonna osa		1	
	Kogu osakond		2	
	Mitu osakonda		3	
	Kogu organisatsioon		4	
	Organisatsioon ja väljaspool		5	
4	**Funktsiooni iga**	1		5
	Üle 10 a		1	
	7 kuni 10 a		2	
	4 kuni 6 a		3	
	1 kuni 3 a		4	
	Alla aasta		5	
5	**Eelmiste auditite leiud**	2		10
	Hiljutine audit: nõrkusi polnud		1	
	Hiljutine audit: oli väikesi nõrkusi		2	
	Pole varem auditeeritud		3	
	Audit: mõned nõrkused		4	
	Audit: palju nõrkusi		5	
6	**Funktsiooni keerukus**	3		15
	Väga väike		1	
	Väike		2	
	Mõõdukas		3	
	Suur		4	
	Väga suur		5	
7	**Töötajate arv**	1		5
	Üks		1	
	Alla 5		2	
	6 kuni 10		3	
	11 kuni 25		4	
	Üle 25		5	
8	**Asukohtade arv**	1		5
	1		1	
	2		2	
	3		3	
	4		4	
	5 või rohkem		5	
	Riski koondhinne			100

15 JÕUSTUMISKUUPÄEV

See protseduur kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. juulil 2002 või pärast seda.

Protseduur P2. Digitaalallkirjad ja võtmehaldus

1. SISSEJUHATUS

1.1 Selle protseduuri eesmärk on anda abivahend sertifitseerimiskeskuse (CA) hindamiseks teenuse osutamise kvaliteedi ja töökindluse aspektides.

1.2 Autentimismeetoditel on oluline roll elektroonilises äris, kus neid kasutatakse juurdepääsu andmiseks firma sisevõrgule või tuvastamaks suhtlus- või tehingupooli (era- või juriidilised isikud). Tehingu- või suhtluspartnerite autentimine, kui seda sobivalt toetab töökindel ja turvaline tehnoloogia-infrastruktuur, on vahend usalduse loomiseks elektroonilises äris.

1.3 Autentimine võib toimuda mitmesugustel turvatasemetel ja põhineda tehnoloogiatel, mis sõltuvad osapoole nõuetest ja tehingu või side omadustest. Inimesed on aastaid kasutanud autentimiseks paroole jt sarnaseid vahendeid, ent tänapäev pakub palju muidki tehnoloogilisi meetodeid, millega hõlbustada seda sidepidamise elutähtsat osa. Tänapäeval saab autentimiseks kasutada mitmesuguseid biomeetrilisi ja krüptograafilistel võtmetel põhinevaid lahendusi nii eraldiseisvatena, omavahel kombineeritult või suurema tehnokeskkonna osana. Paljude ettevõtete arvates on avaliku võtme infrastruktuuril (PKI) põhinevad instrumendid kõige hõlpsamalt mastabeeritavad lahendused äriliseks otstarbeks töökindlate autentimissüsteemide loomisel.

2. TERMINITE JA TEHNOLOOGIA NEUTRAALSUS

2.1 Termin "autentimine" põhineb suurel elektrooniliste rakenduste klassil, mille rollid võivad ulatuda puhtast isikutuvastusest ja volitamisest kuni õigusliku tunnustamiseni.

2.2 Konkreetselt autentimismeetodeid silmas pidades kasutatakse termineid "elektrooniline allkiri" ja "digitaalallkiri" tihti vaheldumisi, mis on tekitanud märkimisväärset rahvusvahelist segadust. Elektrooniline allkiri moodustab funktsionaalse alamhulga üldisemast terminist "digitaalallkiri". Selles dokumendis kasutatavad terminid põhinevad määratlustel, mis on tunnustatud rahvusvaheliste foorumite kaudu saavutanud teatud rahvusvahelise aktsepteeringu.

2.2.1 Paljude autorite määratluses on termin "elektrooniline allkiri" elektroonilisel kujul allkiri, mis on andmesõnumi sisus, tema küljes või temaga loogiliselt seotud, ning mida kasutab isik (või kasutatakse seda tema eest) enda identifitseerimiseks isikutuvastamiseks ning kinnitamaks selle isiku nõusolekut andmesõnumi sisuga.

2.2.2 Seega on digitaalallkiri määratletud kui sõnumile asümmeetrilise krüptosüsteemi rakendamisel saadud teisendus, mis võimaldab isikul, kellel on signeerija sõnum ja tema avalik võti, üheselt kindlaks teha, kas teisendus on loodud salajase võtmega, mis vastab signeerija avalikule võtmele ning kas signeeritud sõnumit on pärast teisendamist muudetud.

2.3 Vahetegemine elektroonilistel ja digitaalsetel allkirjadel on olnud keskmeks rahvusvahelistes aruteludes selle üle, kas poliitikad peaksid tähelepanu osutama elektroonilistele või digitaalsetele allkirjadele. Küsimus on siiani lahtine, mistõttu seda protseduuri võib kohaldada nii elektroonilist kui ka digitaalset allkirja kasutavatele autentimismeetoditele.

Protseduur P2. Digitaalallkirjad ja võtmehaldus (jätkub)

3. DIGITAALALLKIRJADE NING VÕTMEHALDUSE PROTSEDUURID

3.1 Avaliku võtmega krüptograafial põhineva tehnoloogia turvanõuete kontrollimisse kaasatakse usaldatav kolmas pool, keda nimetatakse sertifitseerimiskeskuseks (CA). Sertifitseerimiskeskus levitab elektroonilisi võtmeid, millega krüpteeritakse ja dekrüpteeritakse teavet kasutaja ja serveri vahel; kasutajate ja serverite autentimiseks kasutatakse sertifikaate.

Sertifitseerimiskeskuse (CA) üldine sihtala	**Protseduurid ja nende olemus**
Ettevõtte juhtimine	**Soovitatav(ad) protseduur(id):** Teha kindlaks, kas CA-l on toimiv ettevõttestruktuur, mis võimaldab teabe ja süsteemide toimivat haldust. **Olemus:** Sertifitseerimiskeskuse läbivaatusel tuleb hoolikalt arvestada organisatsiooni aspekte.
Sertifitseerimine/ akrediteerimine	**Soovitatav(ad) protseduur(id):** Teha kindlaks, kas CA on saanud tunnustatud rahvusvaheliselt standardiorganisatsioonilt akrediteeringu turvalise side vallas. **Olemus:** Sertifikaadid ja akrediteeringud, mis sertifitseerimiskeskus on saanud tunnustatud rahvusvahelistelt standardiorganisatsioonidelt, annavad väärtuslikku teavet sertifitseerimiskeskuse toodete ja teenuste kvaliteedi kohta.
Tehnoloogia arhitektuur	**Soovitatav(ad) protseduur(id):** Piiritleda asjakohased ja kohaldatavad standardid (nt X.509-sertifikaatide ja X.500-kataloogide tugi) ning teha kindlaks, kas tehnoloogia arhitektuur põhineb nendel. **Olemus:** Tehnoloogia arhitektuur peaks põhinema standarditel, et tagada usaldusväärsus, mastabeeritavus ja koostalitlusvõime.
Talitluse juhtimine	**Soovitatav(ad) protseduur(id):** Piiritleda sertifitseerimiskeskuse antavad teenused, nt kasutajate registreerimine, võtmete väljastamine ja uuendamine, võtmete varundamine ja taaste, võtmete tühistamine ja taasväljaandmine, võtmete desaktiveerimine ja taasaktiveerimine. Teha kindlaks, kas sertifitseerimiskeskuse teenuste haldamine ja talitlus, välisteenused ning funktsioonisiirded on rahuldavad. Anda mõistlik kinnitus, et on olemas varu-tegevuskoht ja professionaalne tugiteenus .**Olemus:** Talitluse rahuldav juhtimine annab mõistliku kinnituse, et tavad abitegevuste läbiviimiseks on toimivad.

Ülaltoodud meetmete eesmärk on andmete ja dokumentide kogumine ning ettekujutuse andmine sertifitseerimiskeskuse tööst. Järgnev kontroll-loend hõlmab teemasid täpsemalt.

Protseduur P2. Digitaalallkirjad ja võtmehaldus (jätkub)

Sertifitseerimiskeskuse (CA) spetsiifiline sihtala	Protseduurid ja nende olemus
Organisatsiooni haldus	**Soovitatav(ad) protseduur(id):** Teha kindlaks, kas koolituskava on toimiv ja protsessina pidev. **Olemus:** Üks suuremaid turvanõrkusi on teadmiste puudumine. Vaja on liigendatud koolituskava juhtidele ja sertifitseerimiskeskuse käitajatele.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA ühildub standardiga BS 7799 (ISO 17799) või mõne muu standardiga, mis on kohaldatav turvaorganisatsiooni strukuurile. **Olemus:** Turvaorganisatsioonid toetuvad Briti standardile BS 7799 (nüüdisajal ISO 17799), mida vanasti nimetati "Tavade koodeksiks". Kuigi selle sertifikaadi saamine pole kohustuslik, annab nimetatud standardi järgmine mõistliku kinnituse, et poliitikad ja protseduurid on asjakohaselt kavandatud ning töötavad.
Sertifitseerimine/ akrediteerimine	**Soovitatav(ad) protseduur(id):** Teha kindlaks, kas on läbi viidud turvalisuse formaalne hindamine ning saadud sertifikaat. **Olemus:** Paljud riigid nõuavad enne CA turule lubamist, et ta läbiks turvasertifitseerimise vastavalt kohaldatavatele standarditele (nt TCSEC ja ITSEC). Isegi kui seda otseselt ei nõuta, peaksid CA-d kaaluma sellise sertifikaadi taotlemist.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA-l on ISO 9000 kvaliteedisertifikaat. **Olemus:** Mõned riigid nõuavad, et CA-le oleks antud kvaliteedisertifikaat (harilikult ISO 9002). Selline sertifikaat tagab, et sisemised protsessid ja protseduurid on kavandatud ja täide viidud vastavalt hästikavandatud metoodikale, mille eesmärk on paljastamisriski vähendamine.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA-l on avalik käitusjuhend, vastamaks seadusandlusest tulenevatele nõuetele sertifitseerimiskeskuste akrediteerimise osas. **Olemus:** Seadusandlus nõuab sertifitseerimiskeskustelt akrediteeringut. Akrediteeringu taotlemiseks avaldab CA käitusjuhendi, mis täpsustab CA vastutuse ja töö ning reguleerib CA teenuste andmist ja kasutamist.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas sõltumatu kolmas osapool on sertifitseerinud CA turvameetmed, kasutades formaalset riskianalüüsi. **Olemus:** Regulaarsed riskide kaalutlemised, mida sooritab sõltumatu kolmas osapool, kinnitavad CA keskkonna ja töö turvalisust. Tihti tuleneb see juriidilisest nõudest, mis kirjutab CA-dele ette formaalse turvasertifitseerimise.
Tehnoloogia arhitektuur	**Soovitatav(ad) protseduur(id):** Anda mõistlik kinnitus, et CA tarkvara järgib kohaldatavaid rahvusvahelisi standardeid privaatsuse ja turvanõuete osas ning kohalikke nõudeid. **Olemus:** Rahvusvahelised turvastandardid määratlevad nõuded mitte üksnes kogu turva-infrastruktuurile, vaid ka toodetele, mida kasutatakse tundliku teabe kaitsmiseks. Mõnes riigis nõuavad kohalikud õigusaktid kindlate heakskiidetud tarkvarapakettide või krüptoalgoritmide kasutamist.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA toetab eri võtmepaaride kasutamist krüpteerimisel ja digitaalallkirjade andmisel. **Olemus:** Osapooled saavad vastavalt oma vajadustele pidada mitmesugust laadi sidet. Nende sõnumid võivad olla kas signeeritud, krüpteeritud või signeeritud ja krüpteeritud. See eeldab, et võetakse kasutusse eri võtmepaarid krüpteerimiseks ja digitaalallkirjade andmiseks. See on sertifitseerimiskeskuste puhul tihti ainus kohalikes õigusaktides heakskiidetud tööprotseduur.

Protseduur P2. Digitaalallkirjad ja võtmehaldus (jätkub)

	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA annab standarditel põhinevat kataloogiteenust, mis väljastab avalikke võtmeid, sertifikaate ja õigeaegset sertifikaatide tühistamisinfot. **Olemus:** Võimaldamaks juurdepääsu avalikele võtmele, tuleks toetada standarditel põhinevat pöördusmeetodit nagu nt lihtsustatud kataloogisirvimise protokoll (LDAP). Vahel allutatakse LDAP-i struktuur ja talitlus kindlatele nõuetele, et saada mõistlik kinnitus koostalitlusvõime kohta.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas kataloogiteenuse osana pakutakse täiendavat teavet ning kas see mõjutab CA-de koostalitlusvõimet. **Olemus:** Standardne kataloogiteenus väljastab kehtivatele kasutajatele avalikke võtmeid ning sertifikaate. Tüüpiline kataloogiteenus pakub harilikult ka muud teavet, mis võib kasutajaid aidata. Selline täiendav teave pole allutatud ühelegi õigusaktile ning kuulub avaldamisele vastavalt organisatsiooni poliitikale. Oluline on saada mõistlik kinnitus, et see ei mõjuta koostalitlusvõimet (nt sertifikaati, mille on väljastanud üks CA, peab suutma vastu võtta ja verifitseerida suvaline teine CA, millel on seaduslik õigus väljastada sertifikaate).
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA toetab X.509 hetkeprofiile. **Olemus:** Tänapäeval on sertifikaatide struktuuri ainuke tunnustatud standard ITU-X.509 v3. Teiste vormingute kasutamine võib mõjutada sertifitseerimiskeskuste koostalitlusvõimet. Kui CA toetab standardit X.509 v3, saab ta anda paindlikumaid teenuseid ja pakkuda paremat kasutajatuge.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA suudab mõne teise CA väljastatud sertifikaate ära tunda või nende kehtivust kontrollida. Samuti tuleb üle vaadata, kuidas on testitud ristsertifitseerimist, et teha kindlaks CA ja kasutatavate süsteemide tegelik ühilduvus. Võtta arvesse, kas ristsertifitseerimist on kasutatud kusagil mujal töökeskkonnas. **Olemus:** "Ristsertifitseerimine" ehk koostalitlusvõime tähendab CA võimet kontrollida teise CA väljastatud sertifikaatide kehtivust. Mõistagi on ristsertifiseerimine võimalik sama tehnoloogiat kasutavate sertifitseerimiskeskuste vahel, kuid Interneti Tehnilise Operatiivkogu (IETF) töörühm on määratlemas ühiseid liideseid, mis võimaldavad ristsertifitseerimist ka eri tehnoloogiaid kasutavate CA-de vahel. Lisaks on mõnes riigis kehtestatud nõuded ristsertifitseerimiseks (nt krüptoalgoritmid ning sertifikaatide vormingud ja nende levitamispoliitikad).
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas on toetatud alternatiivsetel standarditel põhinevad kehtivuskontrolli-protokollid (nt OCSP). **Olemus:** Teised kehtivuskontrolli-protokollid on muutumas praeguse PKI jaoks hädavajalikuks, nt nõuab Identrus protokolli OCSP. Teised protokollid on koostamisel (nt protokoll DPV ("delegeeritud tee valideerimine")).
Talitluse haldus	**Soovitatav(ad) protseduur(id):** Teha kindlaks, kas eksisteerib võrgupõhine varund, et CA oleks alati kättesaadav. **Olemus:** Isegi kui CA server krahhib, peab organisatsioonile jääma võimalus sertifikaatide kehtivuskontrolliks ja avalike võtmete saamiseks. CA peab tagama nende teenuste katkematu kättesaadavuse.

Protseduur P2. Digitaalallkirjad ja võtmehaldus (jätkub)

	Soovitatav(ad) protseduur(id): Teha kindlaks, kas on toetatud turvaline võtmete varundamine ja taaste. **Olemus:** Juhul kui teave kasutaja võtmete kohta eksikombel kustutatakse või kui kasutaja unustab oma parooli, peaks siiski jääma võimalus võtmete taastamiseks, kui pole toimunud turvariket. Selleks on vaja võtmete turvalist varundamist.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA-l on rahuldav avariitaasteplaan. **Olemus:** Avariitaaste koos toimivate varundamisprotseduuridega annab mõistliku kinnituse, et CA töö jätkub ka juhul, kui tema põhitalitlust tabab katkestus.
	Soovitatav(ad) protseduur(id): Anda mõistlik kinnitus, et privaatsusküsimused on asjakohaselt arvesse võetud ning privaatsuse asjus peetakse kinni kohalikest ja rahvusvahelistest õigusaktidest. **Olemus:** Sertifitseerimiskeskused säilitavad ja haldavad isikuandmeid, mis võivad vahel olla väga tundlikku laadi, nt haiglatele antavad sertifikaadid või sertifikaadid, mis kaitsevad sidet ja tehinguid patsientide ja arstide vahel. Paljud riigid on vastu võtnud konkreetsed seadused, mis kaitsevad inimeste privaatsust tehniliste õigusaktidega; neid seadusi tuleb asjakohaselt arvesse võtta.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA kasutatab kohaliku registreerimisasutuse (LRA) mudelit. **Olemus:** LRA-mudel sätestab, et CA tegeleb sertifikaatide haldamisega ning organisatsioon säilitab kontrolli nende üle, kellel on lubatud sertifikaate saada. Nii vabastatakse ettevõte halduse üldkuludest, jättes talle kohaliku kontrolli turvalisuse üle. Mõnikord on see juriidiline nõue.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA toetab krüpteerimisvõtmete keskset haldamist. **Olemus:** Võtmehaldus hõlmab palju tegevusi: värskendamine, varundamine, taaste, tühistamine, taasväljaandmine, desaktiveerimine ja taasaktiveerimine. Neid tegevusi tuleks sooritada keskselt, et hoida turvalisus kontrolli all. Keskne võtmehaldus aitab säilitada süsteemi terviklust.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA-s on loodud täielikud ja üksikasjalikud poliitikad ja protseduurid. **Olemus:** Tehnoloogiast jääb väheks, et turvalisus oleks mõistlikult tagatud. Äärmiselt tähtsad on ka organisatsioonilised meetmed: poliitikate, protseduuride, standardite ja suuniste dokumenteerimine, tehniline haritus, turvateadlikkus ja juhtkonna heakskiit.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA töö on rollipõhine. **Olemus:** Rollipõhine töö, mis eeldab toimivat kohustuste lahutamist, suurendab turvalisust ja vähendab võimalust sisemise turvarikke tekkeks. Näiteks peaks turvapoliitikate kehtestamisega tegelema teine isik kui võtmete ja sertifikaatide haldamisega.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas võtmed ja sertifikaadid saadakse võrgust, turvaliselt ja läbipaistvalt (seda nii esmaregistreerimise kui ka värskenduste puhul) ning kooskõlas kohaldatavate juriidiliste nõuetega. **Olemus:** Võtmete võrgupõhine haldamine lihtsustab ja kiirendab registreerimisi. Kogu võrgupõhine võtmehaldus (registreerimispäringud, tühistamised ning võtmete ja sertifikaatide levitamine) peab olema täielikult krüpteeritud ja autenditud. Põhiline aspekt on turvalisus, järelikult peab CA võtma kasutusse kõik vahendid, et tuvastada taotleja isik vastavalt seadusele. Seadus määrab tihti (või annab suuniseid), kuidas tuleb võtmete levitamist läbi viia.

	Soovitatav(ad) protseduur(id): Teha kindlaks, kas võtmete sunduuendused (vastavalt organisatsiooni poliitikale) toimuvad turvaliselt ja läbipaistvalt. **Olemus:** Riske saab vähendada, kui kehtestada poliitikad, mis reguleerivad võtmete ja sertifikaatide uuendamise sagedust. Sellised uuendused peavad CA-s toimuma automaatselt, põhinedes organisatsiooni poliitikal, ja olema kasutajale märkamatud.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas võtmed ja sertifikaadid on ajatembeldatud ja arhiveeritud nii, et digitaalseid allkirju saab pikaajaliselt verifitseerida. **Olemus:** Paljud riigid on kehtestanud allkirjastatud dokumentide säilitamiseks konkreetsed nõudmised, nt tuleb finantsdokumente säilitada pettuste avastamiseks vähemalt kümme aastat. CA peaks säilitama võtmete ja sertifikaatide ajaloo ajatemplitega varustatud kujul, et oleks võimalik verifitseerida dokumente, mis on signeeritud ja krüpteeritud minevikus.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas ja kuidas toetatakse tühistamist (nt võrgupõhiselt ja tsentraliseeritult, CRL v2). Teha kindlaks aeg, mis möödub sertifikaadi kuulutamisest kehtetuks ja selle avaldamisest tühistamisnimekirjas. **Olemus:** Kasutaja turvaõiguste tühistamine võib toimuda mitmel põhjusel, näiteks juhul kui kasutaja lahkub organisatsioonist või kui tekib kahtlus, et kasutaja salajane võti või sertifikaat on rikutud. Tühistamist peab olema lihtne teostada ning see peab olema täielik. Tsentraliseerimine võib vähendada aega, mis kulub sertifikaadi tühistamisele. CA-d kasutavad tühistamiseks tühistamisnimekirja (CRL), kuhu haldurid panevad tühistatud serdid. Kasutaja, kelle sertifikaat on CRL-is, ei tohiks ligi pääseda turvatud ressurssidele; see on paljudes riikides kohalike nõuetega ette kirjutatud. Samuti peaks CA toetama CRL v2 (teine versioon standardist, mis reguleerib tühistamisnimekirju). Harilikult ilmub tühistatud sertifikaat CRL-i 24 tunni jooksul.
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA toetab desaktiveerimist ja taasaktiveerimist ning kas tugi on tsentraliseeritud. **Olemus:** Vahel pole kohest vajadust kasutaja turvaatribuutide peatamiseks, nt juhul kui kahtlustatakse turvariket. Võrreldes tühistamisega võimaldab desaktiveerimine kohe takistada turvaatribuutide kasutamist (tühistamine toimub esimesel korral, kui kasutaja või teenus kontrollib CRL-i pärast sertifikaadi sinna panemist).
	Soovitatav(ad) protseduur(id): Teha kindlaks, kas CA säilitab turvaintsidentide kohta auditidokumente. **Olemus:** Turvaline kontrolljälg vähendab turvarikke riski ning turvarikke toimumisel aitab piirata kahjude ulatust.

4. JÕUSTUMISKUUPÄEV

See protseduur kehtib kõikidele IS auditite, mis algavad või toimuvad pärast 1. juulit 2002.

Protseduur P3. Sissetungi tuvastamise süsteemide (IDS) läbivaatus

1. TAUST

1.1 Seosed standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.2 Seosed COBIT-iga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- soorituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jätmise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusse indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

Protseduur P3. Sissetungi tuvastamise süsteemide (IDS) läbivaatus (jätkub)

1.3 Protseduuri vajadus

1.3.1 Protseduuri eesmärk on anda sammud, mida IS audiitorid peaksid järgima sissetungi tuvastamise süsteemi (IDS) läbivaatusel.

1.3.2 See protseduur on kavandatud andma

- IDS-i määratluse ja tööpõhimõtted;
- IDS-i kasutamise eesmärgi ja kasulikkuse;
- IDS-ide põhitüübid ning neist igaühe eelised ja puudused;
- suunised tingimuste kohta, mis peavad olema rahuldatud IDS-i evitamiseks ja haldamiseks;
- IDS-i ülevaatuse plaanimise aspektid;
- ülevaate auditimetoodikast;
- aruandluse aspektid;
- auditiprotseduuride ja auditi asitõendite liigid.

1.3.3 See protseduur määratleb ka IDS-i meetmed COBITi kolmanda väljaande raames, mille on 2000. a avaldanud IT Governance Institute.

2. MIS ON IDS?

2.1 Määratlus

2.1.1 Sissetungi tuvastamine on protsess, mille käigus tehakse spetsiaalse tark- või riistvara abil kindlaks kohalike võrkude või töösüsteemide volitamata kasutamine. IDS-i peaeesmärk on võimaldada võrgus ja süsteemis toimuvate tegevuste nägemist reaalajas ning avastada volitamata tegevused. Lisaks saab IDS sellele automaatselt ja peaaegu reaalajas reageerida. IDS-tooted annavad ka võimaluse analüüsida praegust tegevust varasema tegevuse suhtes, et selgitada välja tähtsamad arengusuunad ja probleemid.

2.2 IDS-i eesmärk ja kasulikkus

2.2.1 Sissetungi tuvastamise peaeesmärk on vältida kahjustusi, mis kaasneksid avastamata jäänud sissetungidega. Toetava turva-infrastruktuuri rajamisel on toimivate turvameetmete programmi evitamine mõjus lähtepunkt. Toimivad meetmed saavad alguse toimivatest infoturbepoliitikatest, standarditest ja tavadest ning asjakohase tehnoloogia kasutamisest. Asjakohane tehnoloogia on määratletud kui tehnoloogia, mis toimivalt toetab ja sunnib täitma organisatsiooni poliitikat. Sissetungi tuvastamise oluline aspekt on suutlikkus sissetungikatseid reaalajas avastada. Käimasolevast rünnakust teadmine ja võimalus sellele kohe reageerida parandab märkimisväärselt võimalust, et sissetungi saab lõpetada ja sissetungikatset jälitada tema allikani. Reaalajas tuvastus sõltub taustal töötavast valvesüsteemist, mis seirab võrku ühendatud seadmete kõiki tegevusi. Seiresüsteem peab suutma tõlgendada mitmesuguseid intsidente ning tuvastada tegelikud rünnakud.

Protseduur P3. Sissetungi tuvastamise süsteemide (IDS) läbivaatus (jätkub)

2.2.2 Paljud tavapärased IDS-id kasutavad rünnakute tuvastamiseks ja kaitseks nende eest võrgu- või hostipõhist meetodit. Mõlemal juhul otsivad IDS-id ründekäekirja ehk spetsiifilisi kujundeid, mis harilikult annavad märku pahatahtlikest kavatsustest või kahtlastest tegevustest. Hästitoimiv IDS peab kasutama mõlemat meetodit.

2.3 IDS-ide põhiliigid

2.3.1 IDS-ide põhiliigid on järgmised:

- Hostipõhised
- Võrgupõhised
    - Statistilise anomaalia meetod
    - Kujutuvastuse meetod

2.4 Hostipõhised IDS-id

2.4.1 Hostipõhine sissetungide tuvastamine sai alguse varajastel 1980ndatel ehk ajal, mil võrgud polnud niivõrd levinud, keerulised ja ühendatud kui tänapäeval. Sellises lihtsas keskkonnas oli levinud tava otsida turvalogidest märke kahtlastest tegevustest. Kuna sissetunge toimus harva, piisas nende tagantjärele analüüsist, et edasised rünnakud ära hoida.

2.4.2 Ehkki hostipõhised IDS-id kasutavad siiani turvalogisid, on nad palju enam automatiseeritud, sest arenduse käigus on neile lisatud keerulisemaid ja tundlikumaid tuvastamismeetodeid. Harilikult seiravad hostipõhised IDS-id süsteemi-, sündmuste- ja turvalogisid. Kui mõni neist failidest muutub, võrdleb IDS uut logi ründekäekirjadega, et teha kindlaks, kas neis leidub vastavusi. Kui jah, siis reageerib süsteem sellele võrguülema hoiatamise ja muude viisidega. Hostipõhise IDS-i peaeesmärk on süsteemide seiramine failides üksikmuudatuste tuvastamiseks.

2.4.3. Hostipõhiste IDS-ide funktsionaalsus on laienenud, haarates teisigi tehnoloogiaid. Üks levinud meetod sissetungide tuvastamiseks on perioodiliselt kontrollida kesksete täidetavate- ja muude failide kontrollsummasid, et leida ootamatuid muudatusi. Reageeringu õigeaegsus sõltub otseselt kontrollimise sagedusest. Viimaks on ka tooteid, mis seiravad tegevust võrguportides ning hoiatavad võrguülemaid, kui keegi pöördub teatud portide poole. See on viis, kuidas võrgupõhist sissetungi tuvastamist saab kasvõi algsel tasemel rakendada hostipõhises keskkonnas.

2.4.4 Hostipõhised IDS-id pole nii kiired kui võrgupõhised, aga neil on siiski eeliseid, millele võrgupõhistes IDS-ides pole vastet. Nende eelised sisaldavad põhjalikumat juurdlusanalüüsi, kitsamat fokuseerimist hostispetsiifiliste sündmuste andmeile ning madalamaid soetamiskulusid.

2.4.5 Hostipõhistel IDS-idel on järgmised eelised.

- Nad teevad kindlaks, kas rünnak õnnestus või nurjus. Olukorras, kus võrgupõhised IDS-id annavad varajase hoiatuse, annavad hostipõhised IDS-id tõenduse, kas rünnak õnnestus või nurjus.

Protseduur P3. Sissetungi tuvastamise süsteemide (IDS) läbivaatus (jätkub)

- Nad seiravad konkreetseid süsteemi tegevusi. Hostipõhised IDS-id suudavad võrku ühendatult seirata kasutajate kõiki tegevusi. Võrgupõhisel süsteemil oleks väga raske esitada sündmusi sellise detailsusega.
- Nad avastavad ründeid, mida võrgupõhised süsteemid ei tuvasta. Näiteks ei pruugi võrgupõhine süsteem tuvastada võrgusisest klaviatuurilt sooritatud rünnet.
- Nad sobivad hästi krüptitud ja kommuteeritavatesse keskkondadesse. Kuna hostipõhised süsteemid paiknevad hostides üle kogu ettevõtte, väldivad nad osasid probleeme, mis tekivad krüptitud ja kommuteeritavates keskkondades paiknevatel võrgupõhistel süsteemidel. Kui on soov tagada ettevõtte laialdane katvus, võib olla raske otsustada, kuhu IDS sisevõrgus täpselt paigutada. Hetkel mil liiklust vaatab läbi hostipõhine süsteem, on andmevoog juba dekrüpteeritud.
- Nad võimaldavad sissetunge tuvastada ja neile reageerida peaaegu reaalajas. Paljud praegusaja hostipõhised süsteemid saavad logifaili uue kirje tekkimisel operatsioonisüsteemilt katkestuse, mille peale saab IDS kirje kohe läbi vaadata. See vähendab märkimisväärselt ajavahemikku ründe avastamisest kuni sellele reageerimiseni.
- Nad ei vaja täiendavat riistvara. Hostipõhised IDS-id paiknevad olemasolevas võrgu-infrastruktuuris, sealhulgas faili- ja veebiserverites ning teistes jagatud ressurssides.
- Nende soetamiskulu on väiksem. Võrgupõhised IDS-id suudavad vähese vaevaga pakkuda laia katvust, kuid on tihti kallid. Hostipõhised sissetungi tuvastamise süsteemid maksavad tihti mõnisada dollarit ühe agendi kohta ning neid saab soetada ka vähese algfinantseerimisega.

2.4.6 Hostipõhiste IDS-ide puudused sisaldavad järgnevat.

- Nende võimekused on rikutud niipea kui hostimasinat tabab turvarike.
- Nad koormavad täiendavalt operatsioonisüsteemi ning neist peab olema koopia igas kaitstavas võrgumasinas.
- Neid võrreldakse tihti viirusetõrjevahenditega, mistõttu kasutajad kalduvad kasutama üksnes viirusetõrjet, ehkki IDS pakub turvavahendeid, mida viirusetõrjetarkvaras ei leidu.
- Nad on väga rakendusespetsiifilised.
- Nad peavad tagama andmevahetuse suurarvuti-operatsioonisüsteemide Windows NT, UNIX, VMS jt vahel, aga sellisel tasemel pakub seda väga vähe IDS-e. Kuna selliste süsteemide osised paiknevad rünnatavas hostis, tekib nutikal ründajal võimalus hostipõhiseid IDS-e rünnata ja blokeerida.
- Nad pole kuigi sobivad, et tuvastada kõikide võrgus paiknevate hostide sondeerimist, kuna iga hosti IDS näeb ainult selliseid võrgupakette, mis on spetsiifiliselt temale suunatud.
- Teenusetõkestusründed häirivad tihti nende võimet töötada ja sissetunge tuvastada.
- Nad tarbivad selle hosti arvutusvõimsust, kus nad töötavad.

Protseduur P3. Sissetungi tuvastamise süsteemide (IDS) läbivaatus (jätkub)

2.5 Võrgupõhised IDS-id

2.5.1 Võrgupõhised IDS-id kasutavad andmeallikana tooreid võrgupakette. Harilikult kasutavad võrgupõhised IDS-id liberaalses režiimis töötavaid võrguadaptereid, millega võrguliiklust reaalajas seirata ja analüüsida. Liberaalne režiim teeb ründeobjekti avastamise ja asukoha määramise häkkerile äärmiselt keeruliseks. Rünnete tuvastamise vahendid kasutavad ründe käekirja äratundmiseks kahte levinud meetodit:

- Statistiliste anomaaliate tuvastamine
- Kujundi, väljendi või baitkoodi vastandamine

2.5.2 Võrgupõhiste IDS-ide eelised sisaldavad järgnevat.

- Nende suurim väärtus on nende varjatus.
- Nende evitamine ei mõjuta olemasolevaid süsteeme või infrastrukuuri.
- Neist enamik on operatsioonisüsteemist sõltumatud. Evitatud võrgupõhised sissetungi tuvastamise andurid panevad tähele kõiki rünnakuid, sõltumata nende sihiks oleva operatsioonisüsteemi tüübist.

2.5.3 Võrgupõhiste IDS-ide puudused sisaldavad järgnevat.

- Nad pole kuigi mastabeeritavad, saades vaevalt hakkama 100 Mbps andmemahtudega.
- Nad põhinevad eelnevalt kindlakstehtud ründekäekirjadel, mis jäävad uutest väheteatud vallutustest alati sammu võrra maha.
- IDS müüjad ei pea sammu kõigi tuntud rünnetega ning annavad ründekäekirjade uuendusi välja harvemini kui viirusetõrjete uuendusi.

2.6 Statistilisel anomaalial põhinevad IDS-id

2.6.1 IDS, mis kasutab anomaaliate avastamise mudelit, avastab sissetungid, otsides märke tegevustest, mis lahknevad kasutaja või süsteemi tavapärasest tegevusest. Anomaalial põhinevad IDS-id rajavad normaalse käitumise võrdlusbaasi, profileerides teatud kasutajaid või võrguühendusi ning seejärel seiravad tegevusi, mis lahknevad võrdlusbaasist.

2.6.2 Statistilisel anomaalial põhinevate IDS-ide eelised sisaldavad järgnevat.

- Nad suudavad paljude turvaasjatundjate arvates avastada senitundmatuid ründeid, erinevalt kujutuvastusel põhinevatest IDS-idest, mis toetuvad minevikus toimunud rünnete käekirja analüüsimisele.
- Nad suudavad avastada ebatavalisi käitumisi ja seega võimaldavad avastada ründeid ilma, et neid peaks selleks spetsiifiliselt programmeerima.

2.6.3 Statistilisel anomaalial põhinevate IDS-ide puudused sisaldavad järgnevat.

- Kuna kasutajate ja võrkude loomus on ennustamatu, väljastavad sellised IDS-id tihti väärtuvastusi.
- Tihti vajavad anomaaliapõhised tuvastamismeetodid normaalsete käitumismustrite kirjeldamiseks ulatuslikke väljaõppekomplekte, mis sisaldavad kirjeid süsteemis aset leidnud intsidentide kohta.
- Hoolikad häkkerid suudavad neist mööduda või need blokeerida.

2.7 Kujutuvastamise meetodit kasutavad IDS-id

2.7.1 Enamik ärikasutuseks mõeldud tooteid põhinevad võrguliikluse uurimisel, et avastada dokumenteeritud ründekujundeid. See tähendab, et IDS on programmeeritud ära tundma (mis võib tähendada ka lihtsalt kujundituvastust) iga teadaolevat vallutusmeetodit. Klassikaline näide on uurida konkreetses võrgusegmendis iga paketti, et leida kindlaksmääratud tegevusmustreid, mis osutaksid katsele pöörduda veebiserveris asuva ohustatud skripti poole. Mõned IDS-id on rajatud suurtele andmebaasidele, mis sisaldavad tuhandeid selliseid kujundeid. IDS seirab kõiki pakette, otsides nende hulgast sellist, mis sisaldaks ühte defneeritud kujunditest.

2.7.2 Kujutuvastamise meetodit kasutavate IDS-ide eelised sisaldavad järgnevat.

- Nende teostamise tähtajad on lühemad kui statistilisel anomaalial põhinevatel IDS-idel. Teisest küljest peab võrgus töötama kujutuvastamise mootor, mis otsib konkreetsete ründemustrite määratlustega sobivaid sündmusi.
- Neid on lihtne teostada, evitada, uuendada ja mõista.
- Nad annavad (võrreldes statistilisel anomaalial põhinevate IDSidega) vähem väärtuvastusi, sest nad annavad suuremal arvul väärignoreeringuid. Teisisõnu on kujutuvastamise IDSid küll kiired, aga neist on lihtsam mööda hiilida.

2.7.3 Kujutuvastamise meetodit kasutavate IDS-ide puudused sisaldavad järgnevat.

- Tavaline võrguliiklus põhjustab palju väärtuvastusi, kuid võrreldes anomaaliapõhiste IDS-idega siiski vähem.
- Hoolikad häkkerid suudavad neist mööduda või need blokeerida.
- Nad ei suuda avastada midagi, mille kohta pole neil kujundit.
- Neid tuleb pidevalt uute reeglitega täiendada.
- Neid on (võrreldes anomaaliapõhiste IDS-idega) lihtsam petta, saates fragmenditud pakette üle võrgu.
- Enamik nende kujundiuuendustest pärinevad IDS-i müüjalt, kellele kanda jääb osa võrgu turvamisest. Kujutuvastuse IDS-ide toimivuse seisukohalt on müüja suutlikkus väljastada äsjaavastatud rünnete kujundeid keskse tähtsusega.

Protseduur P3. Sissetungi tuvastamise süsteemide (IDS) läbivaatus (jätkub)

3. PROTSEDUURID IDS-I TEOSTUSE LÄBIVAATAMISEKS

	Soovitatavad protseduurid
Läbivaatuse plaanimine	Plaanimise lahutamatu osa on ettekujutuse saamine organisatsiooni infosüsteemi keskkonnast määral, mis võimaldab IS audiitoril kindlaks teha süsteemide suuruse ja keerukuse ning selle, mil määral sõltub organisatsioon infosüsteemidest. IS audiitor peaks saama ettekujutuse organisatsiooni missioonist ja tegevuse eesmärkidest, sellest, mis tasemel ja viisil kasutatakse infosüsteeme ja -tehnoloogiat organisatsiooni toeks ning riskidest ja haavatavustest, mis seostuvad organisatsiooni eesmärkide ja infosüsteemidega. Samuti peaks IS audiitor saama ettekujutuse organisatsiooni struktuurist, sealhulgas IDS-i hoolduse eest vastutava IT-personali rollidest ja kohustustest.
	Tuleb koostada ja saada organisatsioonilt kinnitus eesmärkide kohta, mis võtavad arvesse CobiT-i seitset infokriteeriumi. Need kriteeriumid on • toimivus, • tõhusus, • konfidentsiaalsus, • terviklus, • käideldavus, • ühilduvus, • teabe usaldatavus.
IDS-i asetus võrguarhi-tektuuris	Tuleb teha kindlaks kriitiliste varade asukoht võrgus ning koht, millest alates tahab ettevõte tuvastamist rakendada. Näiteks kui organisatsioon tahab läbi vaadata võrguliiklust, mis jääb väljapoole perimeetri marsruuterit, tuleks andur paigadada perimeetri marsruuterist ettepoole. Kui muret tekitab liiklus, mis siseneb võrku perimeetri marsruuterist ja tulemüürist väljaspool, enne elutähtsaid servereid, tuleb andurid evitada selle koha peal. IDS-i paigaldamiskoha kindlaksmääramisel tuleb arvesse võtta järgnevat. • Kas organisatsioon soovib võrguliikluse seiret alustada seespool või väljaspool võrguarhitektuuri. • Andurite paigutamine suure liiklusmahuga võrgusegmenti võib kaasa tuua võrgulatentsi. Võib juhtuda, et tuleb minna kompromissile kaitstuse ja tootlikkuse vahel. • Selleks, et seirata mitmesuguseid nõrkusi ja aidata koormust tasakaalustada, võib võib vaja olla mitmeid andureid. See annab mõistliku kinnituse, et edastatavaid pakette uuritakse põhjalikult, mis parandab sissetungi avastamise võimet. Selle mõiste nimetus on "süviti kaitse". • Millised serverid/rakendused on ohustatud ja mis mõju oleks teenusetõkestusründel (DoS) organisatsioonile? Andurid tuleks paigutada vastavatesse piirkondadesse.

Protseduur P3. Sissetungi tuvastamise süsteemide (IDS) läbivaatus (jätkub)

Paigaldus-parameetrid	Tuleb kindlaks teha järgnev. • Süsteem on seadistatud andmete lükkamiseks analüüsimootorisse või nende sealt tõmbamiseks. Eelistatud meetod on andmete lükkamine. Lükkamist saab seadistada nii, et rünnetest teatatakse analüüsimootorile hetkel, mil need toimuvad. Lükkemeetodi üks puudusi on, et andur saadab vastused ründajatele, mis võib aidata ründajatel anduri olemasolu tuvastada ning korraldada anduri vastu täiendavaid ründeid. Selle nõrkuse leevendamiseks saab andureid seadistada nii, et nad saadavad andmeid analüüsimootorile ka juhul, kui rünnet ei toimu. Tõmbemeetodi puhul saab analüüsimootor anduritelt andmed ning jääb päringuid ootama. Sellises töörežiimis saab ta küll hoiatusi saata, kuid nende sisu teadasaamiseks tuleb teha päringuid. • IDS on seadistatud ära tundma kujundeid ja kasutajate käitumist. IDS tuleks seadistada selliselt, et ta teeks vahet tavalisel ja ebatavalisel võrguliiklusel. See hõlmab süsteemi seadistama tuntud pahaloomuliste käekirjade (nt ussid ja troojalased) äratundmiseks. Näiteks kui IDS tuvastab võrgus välise kasutaja, kelle aadressiruum on sama mis mõnel võrgusisesel kasutajal, peaks see andma ohusignaali, et keegi tüssab võrku. • Kas IDS on varustatud kaughaldusvahenditega.
	Tuleb hinnata IDS-i seadistusparameetreid, et leida nõrku kohti. Teatud parameetrid võivad panna süsteemi või rakenduse krahhima, mis muudab süsteemi kasutuskõlbmatuks.
	Tuleb anda mõistlik kinnitus järgneva kohta. • IDS on seadistatud nii, et ta avastab kahtlased muudatused failides ja andmebaasides või isegi selle, kui on lisatud seletamatuid faile. • IDS seirab kasutajakontosid, süsteemseid faile ja logifaile manipuleeringute avastamiseks. • IDS on seadistatud saatma hoiatusteateid, kui ilmneb kõrgetasemeline sissetung, ning viima miinimumini hoiatusteated, mis tulenevad väärtuvastustest ning madalatasemelistest rünnakutest. • IDS toetub ründekäekirjadele (väärkasutuse avastamine). • IDS saadab hoiatusteateid piiparisõnumi, e-maili või muu vahendiga. • IDS on varustatud aruandlusmooduliga, mis võtab kokku etteantud ajavahemikul (nt tund, nädal, kuu) toimunud rünnakud. • Vastavalt turvapoliitikale on paigaldatud filtrid, mis vähendavad väärtuvastusi.
Suhe tule-müüridesse	Veenduda, et IDS ei vaja tarkvara paigaldamist tulemüüri. Anda mõistlik kinnitus, et sissetungi avastamisele järgnevad asjakohased tegevused. Intsidendile reageerimise protseduurid tuleks välja töötada koos IDS-i teostamisega. Võrgurünnakule vastamise põhimetoodika peaks hõlmama ettevalmistuse, avastamise, ohjeldamise, kõrvaldamise, taastamise ja uue läbivaatuse.
Muud olulised kontrolli-aspektid	Tuleb teha kindlaks järgnev. • Kas mõni töötaja kasutab võrku ühendumiseks lubamatut modemit. • Kas mõni töötaja kasutab illegaalset, turvaohtlikku tarkvara, nt mõnda kaugjuhtimistarkvara nagu Back Orifice. • Kas keelatakse teatud e-maili manused, mis sisaldavad pahatahtlikku koodi, nii et see ei kahanda tööviljakust. • Kas töötajad on kursis URL-idega, mis võivad olla hädaohtlikud, kuna teatud veebilehed on seadistatud vallutama võrku, kust neid sirvitakse. • Kas IDS-i registreeritud intsidentidele reageeritakse korrektselt? Näiteks tuleb kindlaks teha, kas rakendatakse distsiplinaarmeetmeid töötajate suhtes, kes on tabatud võrgus nuhkimiselt ja häkkerivahendite kasutamiselt.

Protseduur P3. Sissetungi tuvastamise süsteemide (IDS) läbivaatus (jätkub)

Audititöö sooritamine	Tuleb dokumenteerida süsteemide töövoog, kogudes selleks teavet nii automatiseeritud kui ka käsitsi teostavate süsteemi aspektide kohta. Fookus peaks olema auditi eesmärgi seisukohalt oluliste andmevoogude töötlusel. Sõltuvalt protsessidest ja kasutatavast tehnoloogiast võib IS audiitor jõuda järeldusele, et tehinguvoo dokumenteerimine ei pruugi olla praktiline. Sellisel juhul peaks IS audiitor ette valmistama üldise skeemi või jutustuse ja/või kasutama võimalusel kvaliteedisüsteemi dokumentatsiooni.
	Tuleb välja selgitada ja testida IDS-i meetmed. Tuleb välja selgitada konkreetsed meetmed, millega leevendatakse riske, ning koguda piisavalt audititõendeid, et teha kindlaks, et need meetmed toimivad ettenähtud viisil. Selle teostamiseks saab kasutada protseduure nagu • küsitlused ja vaatlused; • dokumentatsiooni läbivaatus; • IDS-i meetmete testimine.
	Tuleb kindlaks teha järgnev. • On kolmas osapool, kes annab teavet ja aitab intsidentidele reageerida. • Süsteem suhtleb tulemüüride/marsruuteritega ning see suhtlus on turvatud või toimub eraldi turvaliseks sideks mõeldud kanali või võrgu kaudu (paralleelne juhtimisvõrk). • IDS on varustatud vahendiga, mis tekitab päevaste sündmuste logi põhjal kirjalikke kokkuvõtteid. • Kasutada saab automaatseid reageeringumehhanisme.

Protseduur P3. Sissetungi tuvastamise süsteemide (IDS) läbivaatus (jätkub)

	Tuleb anda mõistlik kinnitus järgneva kohta. • Ründekäekirju uuendatakse tihti. • Uuendusi levitatakse turvalisel viisil (nt krüpteeritult või digitaalse pitseriga varustatult). • IDS suudab avastada paljusid eriliigilisi rünnakuid. • Väärtuvastusi hallatakse sõltuvalt riskiastmest. • IDS vajab reeglite uuendamisi. • IDS-i reeglite andmiseks/uuendamiseks on eraldi isik. • IDS-i ajakohasena hoidmiseks kasutatakse teavet uusimate rünnakute kohta. • IDS on toimivalt mastabeeritav (nt viisil, mis võimaldab paljusid andureid üheaegselt seirata/hallata). • Toode avaldab vähe mõju võrgu/hosti jõudlusele. • On võimalik kontrolli all hoida teisi jõudlusprobleeme, mida IDS tõstatab. • Maksimaalne ribalaius, mida IDS suudab analüüsida ilma kadudeta ning viisil, mis tagab 100% analüüsikatvuse, on kooskõlas organisatsiooni vajadustega. • Kui organisatsioon on võrgupõhine, analüüsib IDS kõiki kasutuses olevaid võrguprotokolle. • IDS on võimeline analüüsima ülakihi rakendusprotokolle küllaldase detailsusega. • IDS ei vaja tarkvara paigaldamist hosti. • Side anduri ja tsentraalse halduri vahel on piisavalt töökindel. • Alarmide hõive on usaldatav. Isegi kui tekitatakse palju alarme, tuleb need kõik hõivata ja andmebaasi talletada. • IDS-ist saadud andmeid hallatakse asjakohaselt ja toimivalt (nt andmete visualiseerimine on keskne aspekt). • On olemas üksikasjalik protseduur selgitamaks ettenähtud tegevusi olukorras, kus IDS on tuvastanud probleemi. • Töötajad saavad aru IDS-i tööpõhimõttest. • IDS-i saab kasutada, et viia läbi muid võrgu haldamise abitegevusi nagu nt võrguseadmete haldamine. • IDS sobib evitamiseks võrgu perimeetris ja ka võrgust väljapool. • IDS avastab sisemised kuritarvitused, mida volitatud kasutajad on korda saatnud pikema perioodi jooksul. • IDS on kohandatud või seadistatud, vastamaks konkreetsetele saidi poliitikatele ja nõuetele. • Nimekiri inimestest, kellel on juurdepääs IDS-ile, on väike ja kontrollitud. • Viiakse läbi koolitusi ning jagatakse asjatundmisi , et IDS paigaldada ja teda käigus hoida ning et perioodiliselt analüüsida tulemusi. • IDS kasutab ära teiste süsteemide tekitatud logisid; • IDS ühildub teiste toodetega, mis kaalutlevad nõrkusi. • IDS suudab rünnakutele reaktiivselt vastata (teavitada tulemüüri/marsruutereid, et blokeerida pakette, mis saabuvad oletatava ründaja IP-aadressilt). • IDS-i aruandlusvahendid on toimivad ja täpsed (sündmuste loetelu, kasutajaliidesed sündmusi kujutavate ikoonidega). • Meetodid, mida kasutatakse IDS-i ülema/turvahalduri hoiatamiseks on tõhusad ja toimivad.
Aruandlus	Nõrkustest tuleb aru anda juhtkonnale. Juhtkonna tähelepanu tuleb osutada IDS-i läbivaatuse käigus avastatud nõrkustele, mis tulenevad meetmete puudumisest või nendega mitteühildumisest. Juhul kui IDS-i läbivaatuse käigus avastatud nõrkused on olulised või kaalukad, tuleb asjakohasel juhtkonna tasemel soovitada kohe rakendada parandusmeetmeid.
	Tuleb mõelda soovituste kaasamisele aruandes, et tugevdada meetmeid.

Protseduur P3. Sissetungi tuvastamise süsteemide (IDS) läbivaatus (jätkub)

4. JÕUSTUMISKUUPÄEV

4.1 See protseduur kehtib kõikidele IS auditite, mis algavad või toimuvad pärast 1. augustit 2003. Täielik sõnaseletuste kogu asub ISACA veebilehel *www.isaca.org/glossary*.

LISA

Toetumine COBITile

Järgnev valik kõige asjakohasematest materjalidest COBIT-is, mida saab rakendada konkreetse auditi ulatuses, põhineb spetsiifiliste COBIT-i IT-protsesside valikul ja COBIT-i teabekriteeriumite arvessevõtmisel.

- PO6 – Teavitada juhtimissihid ja suund
- PO9 – Kaalutleda riskid
- HE3 – Soetada tehnoloogia infrastruktuur ja hooldada seda
- TT5 – Tagada süsteemide turvalisus
- TT7 – Harida ja koolitada kasutajaid
- TT10 – Hallata probleeme

Kõige asjassepuutuvamad kriteeriumid on:

- esmajärjekorras: konfidentsiaalsus, terviklus ja käideldavus;
- teises järjekorras: tõhusus ja usaldatavus.

Protseduur P4. Viirused ja muu kahjurkood

1. TAUST

1.1 Sissejuhatus

1.1.1 Viirusetõrje ja ründeprogrammide poliitika peaks moodustama osa organisatsiooni üldisest turvapoliitikast. See peaks andma ka raamstruktuuri viiruste vältimise, avastamise ja kõrvaldamise protseduurideks.

1.2 Seosed COBITiga

1.2.1 COBITi raamstruktuur määrab: " Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

• sooituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?

• IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?

• teadlikkusele: millised on eesmärkide saavutamata jätmise riskid?

• mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusе indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

Protseduur P4. Viirused ja muu kahjurkood (jätkub)

2. VIIRUSTE JA MUUDE RÜNDEPROGRAMMIDE VÄLTIMINE, AVASTAMINE JA KÕRVALDAMINE

2.1 IS audiitor peaks andma mõistliku kinnituse, et organisatsioonil on viiruste vältimise, avastamise ja kõrvaldamise kohta toimivad dokumenteeritud protseduurid. IS audiitor peaks kasutama järgnevat kontroll-loendit suunisena.

Soovitatavad protseduurid viirusnakkuse vältimiseks ja sellega toimetulekuks
Tuleb üle vaadata juhtkonna analüüs ja kaalutlused elutähtsate ressursside ning evitavate kaitsevahendite kohta. Organisatsiooni viirusetõrjepoliitika peaks põhinema riskide ja turvaaukude kaalutlemisel, et kaitsta organisatsiooni infosüsteeme parimal viisil.
Tuleb läbi viia arutelud IT-talitusega, et tuvastada kõikvõimalikud sisendid arvutisüsteemidesse, nt • füüsiline meedia: disketid, CD-kettad ja irdmeedia üldiselt; • PC-de lisaseadmed: modemid ning seadmed, mis on ühendatud jada-, USB- või infrapunaporti (sh pihuarvutid ja mobiiltelefonid); • kaugühendused sülearvutitest, mis asuvad väljaspool organisatsiooni; • võrguühendused teadaolevate kolmanda osapoole organisatsioonidega nagu nt kliendid, tarnijad ja ametnikkonnad; • organisatsioonis lubatud internetiprotokollid (nt HTTP, FTP ja SMTP). Eriti tuleks tähelepanu pöörata modemitele, kuna kasutajad saavad kasutada sissehelistamisühendusi ilma organisatsiooni teadmata. Näiteks võivad sülearvutid, mis on tihti seadistatud pöörduma kohtvõrkudesse ja Internetti sisemise või välimise modemi kaudu, osutuda viirusekandjateks. Pealegi saab neid modemeid ära kasutada, et anda kasutajatele ligipääs organisatsiooni varadele kontrollimatul viisil. Välised müüjad kujutavad tõsist ohtu, kui poliitikad kolmanda osapoole organisatsioonides on nõrgad või puuduvad.
Tuleb välja selgitada riskid, võttes arvesse võimalikud nõrkused iga platvormi ja iga paigaldatud tarkvara kihi puhul. Seega tuleb arvesse võtta nt operatsioonisüsteemid, teenused (nagu TCP/IP stäkk, meilikontrollijad), e-maili programmid, veebilehitsejad ja muu rakendustarkvara. On mitut laadi koode, mida saab käivitada ja mis võivad valla päästa viirusi (nt teenuse käivitamisel või aktiveerimisel).
Tuleb arvesse võtta organisatsiooni kaalutlus viirusele paljastumise riski kohta (tihti on see tehtud osaks üldisest organisatsiooni riskianalüüsist) ning sellele tuginedes uurida valitud riistvarakomponente ja nendega seotud süsteeme, et teha kindlaks, mis tüüpi faile ja ressursse on lubatud süsteemis käivitada, näiteks • kahjulikud programmid, mis süsteemi käivitamisel laaditakse käivitatavale seadmele; • täidetavad failid, mille käivitab operatsioonisüsteem; • kood, mida interpreteeritakse või käitatakse koos mõne rakendusega (nt DLL-id, Java, VBA); • skriptid ja makrod. Peaks olema sooritatud riskide kaalutlemine, et teha kindlaks, mis failid ja ressursid peaks olema igale süsteemile kättesaadavad. IS audiitor peaks olemasolevaid faile ja ressursse võrdlema vastava riist- või tarkvarastandardiga. Samuti peaks IS audiitor sooritama standardi läbivaatuse kehtestatud parimate tavade suhtes, et teha kindlaks võimalikud nõrkused.
Tuleb läbi vaadata lõppkasutajatele suunatud viirusetõrjepoliitika, kuna eri tüüpi kasutajad võivad käituda erinevalt; samuti võivad neile olla kättesaadavad erinevad ressursid ja meetodid, millega viirust levitada. Viiruse võivad sisse tuua mitmesugused kasutajaklassid nagu • organisatsiooni töötajad; • muu organisatsioonis töötav personal (nt konsultandid, töövõtjad, praktikandid); • inimesed väljaspoolt organisatsiooni, sh kliendid, müüjad ja muud kolmandad osapooled. Selle analüüsi tulemustest on abi organisatsiooni poliitika läbivaatusel, et teha kindlaks, kas see on asjakohane ja pöörab tähelepanu kõigile riskidele, mis on seotud organisatsiooni süsteemide kasutajatega.

Protseduur P4. Viirused ja muu kahjurkood (jätkub)

Tuleb läbi vaadata organisatsiooni võrguarhitektuur, et teha kindlaks võimalikud viiruste levikuteed. • Kõige tavalisemalt levib viirus organisatsioonis kohtvõrkude kaudu. • Serverid võivad viiruseid talletada ja neid levitada, näiteks meilirakenduse kaudu. • E-mail, veebipõhine e-mail, allalaadimised, turvapaikadega varustamata operatsioonisüsteemid ning töötajad või töövõtjad, kes toovad sisse nakatunud kettaid. • Kas kasutatakse e-maili ja tulemüüritehnikaid, et blokeerida teatud tüüpi failid või manused, mis teadaolevalt sisaldavad ründeprogramme. Sellest hindamisest on abi viirusetõrje arhitektuuri läbivaatusel, et teha kindlaks kesksed punktid, kus saab skaneerida viiruseid. On vaja programmi, millega teha poliitika lõppkasutajatele teatavaks ja kasvatada lõppkasutajate teadlikkust.
Tuleb läbi vaadata viirusetõrje poliitika meetmed, mille eesmärk on viirusnakkuse vältimine. See koosneb peamiselt organisatsiooniprotseduuridest ja suhtlusest organisatsiooni sees.
Tuleb läbi vaadata kirjutuspääsu- ja täitmisõigused, samuti operatsioonisüsteemi ja kesksete rakenduste seadistused kasutajate tööjaamades. Poliitika peaks mainima, mis viisil võivad kasutajad sisestada andmeid süsteemi või käivitada programme oma arvutites. Näiteks võib sõltuvalt kasutaja vajadustest olla määratud järgmine. • Irdmeedia kasutamine võib olla blokeeritud. • Teatud liiki failide allalaadimine Internetist (e-maili vahendusel või veebist) võib olla keelatud (nt võidakse filtreerida täidetavaid või Visual Basicu faile). • Makrod võivad olla blokeeritud või eelistatakse makrovabasid dokumente (nt RTF ja CSV). • Kui muutmist pole vaja, saab täielike rakenduste asemel kasutada vaatureid. • Toimub automaatne e-maili viiruste avastamine ja likvideerimine. Igal juhul tuleks hoolikalt paika panna ja läbi vaadata kirjutamispääsu- ja täitmisõigused ning operatsioonisüsteemi ja kesksete rakenduste seadistused kasutajate tööjaamades.
Tuleb läbi vaadata organisatsiooni poliitikad volitamata tarkvara kohta, et teha kindlaks, millised piirangud kehtivad volitamata tarkvara kasutamisele ning kuidas neid piiranguid jõustatakse. Ehkki ideaaljuhul ei saa kasutajad õigust tarkvara omal käel tööjaama paigaldada, on see suutlikkus enamikel juhtudel olemas. Seetõttu peavad organisatsioonil olema meetmed, millega avastada ja kaalutleda riski, et töötajad paigaldavad volitamata tarkvara.
Tuleb kaalutleda riski, et töötajad viivad ründeprogrammi seesmiselt väljatöötatud tarkvarasse. Seda võib saavutada ka toetumisega olemasolevatele protseduuridele, sh vastuvõtutestimisele, mis viiakse läbi eraldi arvutisüsteemil enne tootes evitamist.
Tuleb läbi vaadata müüja infomaterjalid turvaaukude paranduste kohta. Protseduurid peaks tagama, et need parandused on paigaldatud õigeaegselt.
Tuleb kindlaks teha organisatsiooni varundamisstrateegia. Kuna viiruse ilmnemisel võib osutuda vajalikuks taastada süsteemid, rakendused ja/või andmed, peaks poliitika eest vastutav isik tagama, et see strateegia on küllaldane, võimaldamaks viirusepuhangu järel varustust taaskäivitada ilma suuremate andmekadudeta. Kuna enamik viirusi põhjustavad andmekadu tööjaama tasemel, on oluline teavitada kasutajaid poliitikatest ja protseduuridest, mis hõlmavad andmete varundamist tööjaamades.
Tuleb läbi vaadata viirusnakkuse riski leevendavad poliitikad, s.t ennetustegevused nakkuse vältimiseks nagu • ohtu kujutavate dokumentide ja failide liigid, • e-mailidega seonduvad riskid, • kasutatavate süsteemide kahtlasest käitumisest aru andmine. Kasutajatel on tähtis osa viiruste vältimise jõupingutustes. Kasutajate üks rolle on võimalike nakkusallikate avastamine.
Tuleb läbi vaadata organisatsiooni tegevused oma riskide kaalutlemiseks ja leevendamiseks juhul kui ta levitab viiruseid teistele. Väljuvate e-mailide lõppu ning lepingutesse, mis sõlmitakse üksusega, kellega organisatsioon vahetab andmeid, tuleb lisada lausungid, mis piiravad organisatsiooni vastutust.
Tuleb kindlaks teha, kas viirusetõrjetarkvara poliitika on selgelt määratletud ja kohaldatud. Ehkki vältimine on viirusetõrjepoliitika tähtis osa, on oluline viiruste tõhus avastamine kohe, kui nad satuvad süsteemidesse.

Protseduur P4. Viirused ja muu kahjurkood (jätkub)

Tuleb hinnata viirusetõrjetarkvara nelja viiruste kontrollimise koha suhtes: • kasutaja tööjaama ressursid, nt flopikettad, kõvakettad ja irdmeedia; • failiserverid: sisenevad ja väljuvad failid; • meilirakendused: manused, sh täidetavat koodi sisaldavad; • Interneti-lüüsid: sisenev andmevoog (protokollid SMTP, HTTP, FTP) ja aktiivsed komponendid (nt Java ja ActiveX). Poliitika peaks kirjeldama, mis laadi viirusetõrjetarkvara tuleb paigaldada igasse ohtude analüüsi käigus väljaselgitatud punkti. Näiteks arvuti, mis pöördub Internetti teenusepakkuja vahendusel, peaks olema kohalikult kaitstud, et avastada viirused enne nende levimist.
Tuleb läbi viia viirusetõrje pakkujate tüüptehniline analüüs ja hinnata nende protseduure ründeprogrammide kohta. Muuhulgas tuleb arvesse võtta järgnevat. • Kui tihti väljastatakse definitsioonide uuendusi. • Kui kiiresti levitatakse eriuuendusi, kui ilmneb suurem puhang. • Mis vahenditega ja kui kiiresti annab müüja teada uutest ohtudest. • Milliseid haldusvahendeid pakutakse, et hõlbustada evitamist ja uuendamist. • Mis laadi tuge pakub müüja viirusepuhangu korral. Sõltuvalt ohuanalüüsi tulemustest ja organisatsiooni keerukusest saab valida viirusetõrje erinevatelt müüjatelt. Näiteks kui paigaldada üks viirusetõrjeprogramm kasutaja-tööjaamadesse ja teine meiliserveritesse, võib see maksimeerida viiruste avastamise võimalust, eriti kui need viirusetõrjeprogrammid kasutavad eri tehnoloogiaid. Samas peab organisatsioon haldama kasvanud keerukust, mis tuleneb uuenduste saamisest mitmelt viirusetõrjemüüjalt.
Tuleb kindlaks teha, kas organisatsioon on kaalutlenud täieliku skaneerimise tehnoloogia kasutamist sellega kaasneva tööviljakuskao suhtes. Tuleb kontrollida, kas organisatsioon on teinud sellise analüüsi ja asjakohaselt arvesse võtnud selle tulemuse (kui täieliku skaneerimisega kaasnev kadu tööviljakuses on vastuvõetamatu, kalduvad kasutajad viirusetõrjetarkvara oma süsteemides blokeerima või sellest mööda hiilima, mis suurendab paljastamisriski). See poliitika määrab, mis laadi skaneerimist tuleb kohaldada sõltuvalt arvesse võetavast ressursist ja hinnangust ohule. See peaks määrama, kui tihti või mis tingimustel tuleks käivitada nõudepõhine viirusekontroll, kuna pöördusepõhised kontrollid tarbivad palju arvutusvõimsust.. Näiteks tuleb loetleda skaneeritavad failitüübid. Harilikult pakuvad viirusetõrjeprogrammid kahte liiki skaneerimist: • Pöördusepõhine: viirusetõrjetarkvara seirab reaalajas ja kasutaja sekkumiseta kõiki andmeid, mille poole pöördutakse; see peaks pidevalt töötama vähemalt failiserverites, meiliserverites ja Interneti-ressurssides. • Nõudepõhine: viirusetõrjetarkvara tuleb ise käivitada, et kontrollida teatud ressurssi ettenähtud ajal. • Tuleks mõtelda ka teistele skaneerimisprotseduuridele. Näiteks on mõnes organisatsioonis server, mis skaneerib paljusid teisi, selle asemel, et laadida viirusetõrjetarkvara paljudesse arvutitesse. Sedatüüpi otsing töötab koostöös "aktiivse" skaneerimisega.
Tuleb läbi vaadata organisatsiooni protseduurid viirustejuhtumitest aru andmise kohta. See peaks sisaldama, kellele organisatsioonis antakse aru viiruse avastamisel (nt konsultatsioonipunkt, viirusetõrje operatiivkogu), intsidendile reageerimise protseduure ja aruandlust juhtumite kohta. Viiruse leidmisest organisatsioonist tuleks kohe teatada ning organisatsioonil peaks olema selleks puhuks asjakohased reageerimisprotseduurid. Need peaks sisaldama spetsifikatsioone järgimisele kuuluvate protseduuride kohta; piiranguid isikutele, kes tohivad kasutaja-tööjaamadesse paigaldatud viirusetõrjetarkvara blokeerida või selle sätteid muuta, ning eskaleerimise ja aruandluse protseduure.
Tuleb anda mõistlik kinnitus, et viirusetõrjetarkvara uuenduste sagedus ja skoop vastavad viirusetõrjetarkvara toimetaja soovitustele, organisatsiooni poliitikale ja riskile, mis seondub iga IT-keskkonnaga. Uuendusi on tavaliselt kahte sorti: • mootori uuendused, mille käigus muudetakse viirusetõrjetarkvara tuuma; • viirusedefinitsioonide uuendused, mis väljastatakse uute viiruste avastamisel.
Tuleb anda mõistlik kinnitus, et enne töökeskkonnas evitamist läbivad viirusedefinitsioonid ja viirusetõrjemootori uuendused testimise eraldi arvutisüsteemil, sarnaselt muude tarkvarauuendustega. Mõned toimetajad väljastavad suurema viirusepuhangu ilmnedes ka definitsioonide hädauuendusi; vaja on protseduuri, millega saab juhtkond kohe nendest uuendustest teadlikuks ja saab need kiiresti evitada (pärast asjakohast testimist). Paljud viirusetõrjetooted nii tööjaamadele kui ka serveritele on varustatud automaatuuenduse võimalusega. Sellele funktsioonile tuleks mõelda, kuna suurtes võrguga kaetud süsteemides, kus on palju servereid ja tööjaamu, võib uuenduste käsitsi paigaldamine olla töömahukas ettevõtmine.

Protseduur P4. Viirused ja muu kahjurkood (jätkub)

Tuleb anda mõistlik kinnitus, et IT-personal seirab asjakohaselt viirusetõrje uuenduse olekut täielikkuse ja täpsuse suhtes – üksainus uuendamata tööjaam võib kujuneda viirusepuhangu lähtepunktiks. Kohtvõrgu keskkonnas paigaldab viirusetõrje uuendusi serveritesse alati IT-personal. Seevastu paigaldused klientarvutitesse/tööjaamadesse delegeeritakse tihti kasutajatele.
Tuleb anda mõistlik kinnitus, et on olemas poliitika, mis hõlmab vahendite (nt tulemüürid) kasutamise viirusetõrjestrateegias. Vahendid pole mõeldud otseselt viirustega tegemiseks, kuid nende abil võib avastada troojaviirusi, kui nood aktiveeritakse. Teised tarkvaratooted suudavad avastada meilirakenduste kahtlast käitumist.
Tuleb läbi vaadata protseduurid, mis on kavandatud viirusepuhangu peatamiseks ning nakatunud ressursside parandamiseks juhul, kui viirusetõrjetarkvara ei avasta ega kõrvalda viirust. (Nt võib osutuda vajalikuks serverite seiskamine ja/või füüsiliste võrguühenduste lahtiühendamine.) Need protseduurid tuleks käivitada alati, kui tekib viirusnakkuse kahtlus. Poliitika peaks üksikasjalikult kirjeldama meetmed, mis tuleb ette võtta puhangu peatamiseks. Sõltuvalt viiruse liigist võib osutuda vajalikuks mõne rakenduse (näiteks meilirakenduse või failiserveri) peatamine. Vajadusel saab isoleerida osa organisatsiooni võrgust. Viirus võib olla süsteemi sisenenud kas avastamismeetmeid vältides või seetõttu, et tema definitsioon polnud veel kirjas viirusetõrjetarkvara andmebaasides. Seepärast peab poliitika määratlema, et viirusedefinitsioonide uuendamise järel tuleb käivitada nõudepõhine kontroll. Juhul kui viirus jääb ikka avastamata, võib kahtlased failid saata viirusetõrje müüjale ülevaatuseks.
Tuleb anda mõistlik kinnitus, et viiakse läbi kahjude kaalutlemine, millega tehakse kindlaks süsteemide osad, mida puhang mõjutas. Keskkondade, programmide ja/või andmete taastamiseks võib kasutada varukoopiaid. Pärast viirustõrjetarkvara uuendamist, et ta tuleks toime uue viirusega, võib süsteemi taaskäivitada. Tuleb anda mõistlik kinnitus, et varu- ja taastefailid pole viirusega nakatunud.
Tuleb läbi vaadata organisatsiooni teavitus- ja hoiatusprotsessid, et kaalutleda, kas puhangud on tehtud teatavaks teistele organisatsiooniüksustele, kuna ka nemad võivad olla nakatunud. Poliitika peab kirjeldama viisi, kuidas see teave edastatakse õigeaegselt asjakohastele partneritele.
Tuleb anda mõistlik kinnitus, et viirusetõrjepoliitika on põhjalikult dokumenteeritud ning on kirjutatud protseduurid, millega evitada seda üksikasjalikumalt. Protseduurid, mis pole korralikult dokumenteeritud, on mittetoimivad.
Tuleb anda mõistlik kinnitus, et on kehtestatud poliitikad ja protseduurid, millega reguleeritakse formaliseeritud viirusetõrjepoliitikat toetava dokumentatsiooni asjakohast hoiuleandmist ja säilitamist. Dokumentatsiooni tuleb säilitada, et tagada nõuetekohane uus läbivaatus.
Tuleb saada mõistlik kinnitus, et kasutajad on läbinud koolituse (sh õpitud materjali kontrollimise) viirusetõrje turvapoliitika protseduuride osas. Pärast õnnestunud teadmiste kontrolli peaks kasutajad alla kirjutama dokumendile, mis kirjeldab nende rolle poliitika piires. Kasutajaid tuleb teavitada viirusetõrje turvapoliitikast, kasutades vahendeid nagu • esitlused töötajate koosolekutel, • teavitused meili teel, • turvateadlikkuse veebileht.
Tuleb läbi viia regulaarsed kaalutlemised protseduuri kohaldamise ja tema toimivuse kohta, võttes arvesse järgnevat: • poliitika dokumenteeritus, • ohuanalüüs, • nakkuste vältimine, • nakkuste avastamise vahendid, • nakkuste kõrvaldamine. Poliitika kaalutlemiste ja organisatsiooni arengu tulemused tuleks regulaarselt läbi vaadata ja kasutada neid viirusetõrjepoliitika uuendamisel.

Protseduur P4. Viirused ja muu kahjurkood (jätkub)

3. MEETODID VIIRUSTE JA MUU KAHJURKOODI KOHTA KÄIVATE POLIITIKATE JA PROTSEDUURIDE TOIMIVUSE KAALUTLEMISEKS

3.1 Soovitatavad meetodid

Soovitatavad meetodid, millega kaalutleda viiruste ja muu kahjurkoodi kohta käivate poliitikate ja protseduuride toimivust
Tuleb hinnata ennetavate meetmete kasutamist, sh järgnevat: operatsioonisüsteemide hooldus koos kõigi paigaldatud paikade ja parandustega; sisu filtreerimist lüüsides; üleettevõtteline turvateadlikkuse programm, sh meeldetuletused ja järgnevad programmid; manuste (nagu .exe, .com, .vms) mahavõtmine; "liivakasti"-metoodika kasutamine; veebipõhistele e-mailisaitidele ligipääsu piiramine tulemüüri või töölaua tasemel; Internetist failide allalaadimise blokeerimine, v.a juhtudel, mis õigustavad vajadust.
Tuleb saada ettekujutus käesolevast võrgu-infrastruktuurist (võrgu arhitektuur ja tehniline lahendus), kasutades seda dokumenteerivaid võrguskeeme.
Tuleb kindlaks teha, kas on välja selgitatud igat tüüpi PC-d, pihuarvutid, failiserverid, e-maili lüüsid, Internetti ühendumise punktid, peamised tarkvaraliigid, kaugasukohad ning WAN-, VAN- ja VPN-ühenduvusplatvormid.
Tuleb välja selgitada võimalikud viiruste sisenemispunktid, sh e-maili süsteemid, allalaadimised, nakatunud flopikettad, operatsioonisüsteemidele paigaldamata jäänud turvaparandused ning igasugused ärajäänud tarkvaratestimised eraldi arvutisüsteemil enne ükskõik millise tarkvara võrku paigaldamist.
Tuleb välja selgitada, millist viirusetõrjetarkvara kasutatakse, kuidas see teeb kindlaks failide nakatumise ning kuidas see lahendab (teavituste, paranduste, karantiini panekutega) sellised juhtumid igal platvormil/keskkonnas (nt tulemüür, UNIX, PC).
Tuleb saada ja läbi vaadata kõik ründeprogrammidesse puutuvad protseduurid, sh järgnevad aspektid. • Defineerimine ja levitamine; • Teadlikkuse tõstmise koolitused kasutajatele, võrgu- ja süsteemihalduritele ja konsultatsioonipunktide analüütikutele, kus selgitatakse tarkvara kasutamist, viiruste levitamise vältimise ning protseduure, mis tuleb läbi viia viirusekahtluse korral; - Kasutajad peavad PC-d vähemalt iganädalaselt peatama, kui viirusetõrjetarkvara uuendamine seda nõuab; - Kasutajad ei saa oma arvutis blokeerida viirusetõrjetarkvara; • Äsjaostetud tarkvara või selle uue versiooni evitamine; • Süsteemse ja rakendustarkvara paikade ja paranduste evitamine; • Viirusetõrjetarkvara hooldatakse jooksvalt; • Turvapoliitikad kõigi süsteemi kontode jaoks (nt haldur, külastaja); • Turvapoliitikad kõigi kontode/identiteetide jaoks (nt paroolide pikkus, paroolide regulaarne vahetamine, paroolide ajalugu, aegumisperiood, lukustamine, parooli tugevus); • Tüüpnõuded võrgu seadistamisele (võimalusel saab kasutada ettevõtte seadistuste haldamise vahendit); • Tüüpnõuded rakendustele; • Tüüpnõuded e-mailile; • Vastutuste määramine nende poliitikate ja protseduuride kohaldamiseks.

Protseduur P4. Viirused ja muu kahjurkood (jätkub)

Tuleb läbi viia spetsiaalsed testid turvaaukude ja turvariskide hindamiseks, näiteks: • valida välja mõned võrgukettad ning kontrollida neid viirusetõrjetarkvaraga, et teada saada, kas mõnes võrguserveris on nakatunud faile; • vestelda NT halduriga teenustest, mis töötavad NT serveris ning põhjustest, miks seda peetakse asjakohaseks; • võtta juhuvalik PC-sid ja sülearvuteid ning kontrollida, et viirusetõrjetarkvara on asjakohaselt ja rahuldavalt paigaldatud ning sellest on kasutuses uusim versioon; samuti, kontrollida, et kasutaja ei saa ega pole viirusetõrjetarkvara blokeerinud; • teha kindlaks, kas on laaditud uusim versioon viirusesignatuuridest; • võtta juhuvalik PC-sid ja sülearvuteid ning kontrollida viirusetõrjetarkvaraga, kas mõnes PC-s on nakatunud faile; • küsitleda lõppkasutajaid viirusetõrjepoliitika teadmise kohta; • saada kolmanda osapoole viirusetõrjepoliitika ja -seadistused ning hinnata nende asjakohasust.
Tuleb kindlaks teha aruandekohuslus ja õigeaegsus, et kehtestada protseduurid, mis on vastuolus.
Tuleb anda mõistlik kinnitus, et intsidendi käsitlemise protseduurid on määratletud ja kasutuses.
Tuleb läbi vaadata dokumentatsioon valitud ajavahemikul ilmnenud intsidentide kohta, et kindlaks teha järgnev. • Asjakohaseid juhte informeeriti. • Üksikasjad dokumenteeriti. • Levik viidi miinimumini. • Intsidendiaruanded tehti teatavaks teistele kasutajatele. • Viirused kõrvaldati. • Intsidente uuriti. • Intsidente käsitleti asjakohaselt. • Tehti ettevalmistused juhtumi kordumise puhuks. • Võrku seirati ebatavaliste tegevuste suhtes.
Tuleb läbi vaadata viiruse eemaldamise protsess, mis peaks sisaldama järgnevat: Inteneti-ühenduse katkestamine, skaneerimis- ja avastamisvahendite kasutamine, käivitamisfailide kontrollimine, mälu kontrollimine, troojaviirusele avatud portide otsimine ning troojaviirusega nakatunud failide ning e-mailiusside kustutamine.
Juhul kui hiljuti pole läbi viidud turvaauditit, tuleb läbi vaadata kõikide kontode/identiteetide õigused kõrgete privileegide leidmiseks, et anda mõistlik kinnitus, et need on antud üksnes neile, kelle töökohustused nõuavad sellist pääsutaset. Samuti tuleb anda mõistlik kinnitus, et sellised privileegid nõuavad tugevaid paroole ja teisi sarnaseid meetmeid (nt piiratakse ligipääsu võimsatele töövahenditele).

4. ARUANDLUS

4.1. Nakkusekahtlus

4.1.1. Iga kasutaja vastutab omaenda varade (s.t arvuti ja lisaseadmete) eest. Kui kahtlustatakse ründeprogrammi põhjustatud nakkust, peaks kasutaja kohe lõpetama töö arvutiga ja järgima juhtkonna ja/või turvaülema antud hädaprotseduure. Lisaks peaks ta probleemist teavitama asjakohaseid osapooli (turvaosakond, konsultatsioonipunkt jms), et leevendada tagajärgi ning vähendada ründeprogrammide leviku tõenäosust organisatsioonis. Kui kasutajal pole võimalik protseduuri järgida, peaks ta kohe arvuti välja lülitama ja küsima abi asjakohaselt osapoolelt (turvaosakond, konsultatsioonipunkt jms).

Protseduur P4. Viirused ja muu kahjurkood (jätkub)

5. JÕUSTUMISKUUPÄEV

5.1 See protseduur kehtib kõigile IS auditite le, mis algavad või toimuvad pärast 1. augustit 2003. Täielik sõnaseletuste kogu asub ISACA veebilehel *www.isaca.org/glossary*.

LISAD

Järgnev valik kõige asjakohasematest materjalidest COBITis, mida saab rakendada konkreetse auditi ulatuses, põhineb spetsiifiliste COBITi IT-protsesside valikul ja COBITi teabekriteeriumite arvessevõtmisel.

- PO6 – Teavitada juhtimissihid ja -suund
- PO9 – Kaalutleda riskid
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- HE6 – Hallata muutusi
- TT4 – Tagada pidev teenus
- TT5 – Tagada süsteemide turvalisus
- TT10 – Hallata probleeme

Kõige asjassepuutuvamad teabekriteeriumid on

- esmajärjekorras: terviklus ja käideldavus;
- teises järjekorras: konfidentsiaalsus ja usaldatavus.

Protseduur P5. Juhtimisriski isehindamine

1 TAUST

1.1 Seos ISACA standarditega

1.1.1 Standard S5 "Plaanimine" määrab: "IS audiitor peaks plaanima infosüsteemide auditi katvuse nii, et see hõlmaks auditi eesmärke ning vastaks kohaldatavatele õigusaktidele ja kutsealastele auditeerimise standarditele."

1.1.2 Standard S6 "Auditi tööd sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.3 Standard S7 "Aruandlus" määrab: "Pärast auditi lõpuleviimist peaks IS audiitor koostama sobivas vormis aruande. Aruandesse tuleks märkida organisatsioon, eeldatavad saajad ja võimalikud levituskitsendused. Auditi aruanne peaks teatama sooritatud auditi töö käsitlusala, eesmärgid, hõlmatud perioodi, ajastuse ja ulatuse. Aruanne peaks teatama leiud, järeldused ja soovitused ning kahtlused, piirangud või käsitlusala kitsendused, mis IS audiitoril võivad olla auditi suhtes. IS audiitoril peaksid aruandes esitatud tulemuste toetuseks olema piisavad ja asjakohased auditi asitõendid. Väljastamisel tuleks IS audiitori aruanne varustada allkirja ja kuupäevaga ning levitada vastavalt auditi põhikirja või töövõtukirja tingimustele."

1.1.4 Standard S8 "Järeltoimingud" määrab: "Pärast leidude ja soovituste teatamist aruandes peaks IS audiitor taotlema asjakohast teavet ja hindama seda otsustamiseks, kas juhtkond on õigel ajal rakendanud asjakohaseid meetmeid."

1.1.5 Juhiseid annab suunis G13 "Riski kaalutlemise kasutamine auditi plaanimisel"

1.2 Seos COBITiga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- sooritusele mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jäämise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusindikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise seminaride toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

1.2 Protseduuri vajadus

1.2.1 See protseduur on kavandatud andma

- IS auditi juhtimisriski isehindamise (CRSA) määratluse;
- juhiseid CRSA metoodika kasutamise kohta;
- juhiseid CRSA teostamise kohta.

2 CRSA

2.1 CRSA määratlus

2.1.1 CRSA on kasulik meetod või protsess, millega juhtkond ja kõigi tasemete personal abistaja suunamisel kollektiivselt tuvastab ja hindab infosüsteemidega seotud riske ja juhtimismeetmeid; abistajaks võib olla IS audiitor. See IS audiitor saab CRSA-d kasutada riskidesse ja juhtimismeetmetesse puutuva teabe kogumiseks ning juhtkonna ja personaliga tehtava koostöö tugevdamiseks. CRSA asemel võib kasutada termineid "juhtimisriski isehindamine" ja "riski ja juhtimise isehindamine". CRSA annab juhtkonnale ja töötajaile raamstruktuuri ja instrumendid, millega

- piiritleda ärieesmärgid ja anda neile prioriteedid;
- hinnata ja hallata äriprotsesside suureriskilisi alasid;
- ise hinnata juhtimismeetmete adekvaatsust;
- töötada välja riski käsitlemise tegevusplaane;
- tagada, et organisatsiooni kõigil tasemetel on ärieesmärkide ja riskide piiritlemine, tundmine ja hindamine järjekindel.

2.2 Eesmärk

2.2.1 CRSA on meetod, mis lisab väärtust sel teel, et suurendab majandusüksuse osalust juhtimis- ja riskisüsteemide kavandamises ja käigushoius ning riskile avatud kohtade tuvastamises ja parandusmeetmete otsustamises. CRSA protsessilt saavad tuge IS auditeerimise standardid "Plaanimine", "Audititöö sooritamine" ja "Aruandlus".

2.3 IS audiitori osalemine

2.3.1 IS audiitori osalemine CRSA üritustes võib olla märkimisväärne ning võib hõlmata CRSA protsessi spondeerimist, kavandamist, rakendamist ja sisuliselt ka haldamist, CRSA koolituse läbiviimist, abistajate andmist, keskse juhtkonna ja personali osalemise orkestreerimist ning CRSA tulemite ülesmärkimist ja teatamist. Teisal võib IS audiitori osalemine CRSA üritustes olla minimaalne, audiitor võib olla kogu protsessi puhul üks huvipool ja konsultant ning töörühmade sooritatud hindamiste lõplik kontrollija. Enamasti on IS audiitori osalemine CRSA üritustes kusagil nende kahe äärmuse vahel.

2.3.2 Milline ka ei oleks IS audiitori roll CRSA protsessis, säilitab audiitor kutsealase sõltumatuse ja objektiivsuse vastavalt standardile S2 "Sõltumatus" ja suunisele G12 " Organisatsiooniline seos ja sõltumatus". Harilikult tegutseb IS audiitor abistajana, toetudes riskide tuvastamisel ja hindamisel ning tegevusplaanide väljatöötamisel tegevusliini juhtkonnale ja personalile. IS audiitori panus on ta asjatundmine sisemeetmete hindamise, teostamise ja toimivuse alal, täpselt nii nagu muudegi auditeerimismeetodite puhul. Tegevusliini juhtkonna vastutusele jäävad sisemeetmete toimiv kasutamine ning otsuste kaalutlemine ja tegemine nõuannete põhjal, mida ta saab CRSA aruande ja pakutava riskihalduse tegevusplaani kujul.

2.3.3 CRSA üritus laiendab IS audiitori traditsioonilist rolli sellega, et ta aitab juhtkonnal täita oma kohustusi riskihalduse ja -ohje protsesside rajamise ja käigushoiu alal ning selle süsteemi adekvaatsuse hindamise alal. CRSA ürituse kaudu teevad IS audiitor ning allüksused ja talitused koostööd parema teabe saamiseks selle kohta, kui hästi töötavad juhtimisprotsessid ja kui olulised on jääkriskid.

2.3.4 CRSA-d ei tuleks vaadelda traditsioonilisemate auditeerimismeetodite asendajana, vaid teda tuleks arvestada ühe instrumendina üldises IS tagamise ja auditeerimise raamstruktuuris, mis hõlmab CRSA, traditsioonilised auditeerimismeetodid, aruandluse ja järeltoimingud.

2.3.5 Kui CRSA üritus on läbi viidud siseauditi talitusest sõltumatult või kui IS audiitori osalus on olnud minimaalne, on soovitatav, et IS audiitor vaataks läbi CRSA tulemid; see aitaks valideerida riski kaalutlemisi ja pakutud tegevusplaane ning aitaks ka tagada, et IS audiitor hoiab end ajakohaselt kursis vaatlusaluse ala või talituse riskiprofiiliga.

2.4 CRSA hüved ja eelised

2.4.1 CRSA püüab integreerida riskihalduse tavasid ja kultuuri sellega, kuidas personal täidab oma tööülesandeid ja allüksused saavutavad oma eesmärke. CRSA edukal rakendamisel on rida häid külgi; ta

- kaasab auditi kliendi otseselt riski kaalutlemise ja juhtimise hindamise tegevustesse ning aitab seeläbi luua kliendi ja IS audiitori vahel partnerlussuhte;
- võimaldab IS audiitoril paremini eraldada nappe ressursse, kaasates kliendi riski kaalutlemise ja juhtimise hindamise protsessi;
- harib juhtkonda ja töötajaid riskihalduse ja juhtimise hindamise alal;

- viib allüksuse eesmärgid kooskõlla kogu organisatsiooni sihtidega;
- arendab riskide ja juhtimismeetmete omanduse tunnet;
- arendab riski käsitlemisel rühmatööd;
- täiustab suhtlust allüksuste vahel ja kogu organisatsiooni ulatuses;
- annab mehhanismi, millega tõsta juhtkonna ja personali teadlikkust sellest, kuidas võivad üleorganisatsioonilise juhtimissüsteemi üldist tervislikku seisundit mõjutada pehmed meetmed, näiteks organisatsiooni väärtused, eetikanormide pädevus ja juhtimisstiilid.

2.5 CRSA piirangud

2.5.1 CRSA ei ole meetod pettuste leidmiseks ja ta ei tarvitse sobida regulatiivseteks audititeks, mis nõuavad atribuutide ja nende dokumentatsiooni kontrollimist.

2.5.2 Teatav juhtimisstiil võib tähendada seda, et küsimuste tõstatamisel arutamiseks ei ole osalejad võib-olla avameelsed riskide paljastamise mõttes, ei usalda üksteist ega tööta toimivalt ühe meeskonnana.

2.5.3 CRSA toimib hästi edasiantava juhtimise ja võimuga organisatsioonikeskkonnas. Ta ei toimi hästi organisatsioonis, mis ei väärtusta uuendust ja koostööd.

2.5.4 Raskusi võidakse kogeda katsetes rakendada organisatsioonis uusi juhtimistavasid, -meetodeid või -kontseptsioone. CRSA protsess toob kaasa algseid ja pidevaid investeeringuid ja seetõttu ei ole ta tasuvust kerge määrata.

2.5.5 Mõned CRSA ürituste sooritamise suuremad tõkked, kitsendused ja ootamatud raskused on järgmised:

- tippjuhtkonnapoolse toetuse puudumine;
- selliste abistajate valimine, kellel pole oskusi ega kogemusi abistamise, konsensusekeskseteмeetodite ning juhtimismeetmete teooria ja rakendamise alal või kes ei valmistu adekvaatselt CRSA seminariks ega tutvu läbivaadatava süsteemiga;
- eduka seminari või seminaride sarja käivitamiseks vajaliku investeeringu, õppimise või plaanimise alahindamine;
- vaatevälja kitsendamine ning seeläbi CRSA ürituse toimivusvõimaluste piiramine;
- alustamine liiga suure esimese projektiga.

2.6 Võimalikud CRSA protsessi jaoks sobivad IS alad

2.6.1 CRSA-d saab kasutada paljudel aladel, sealhulgas süsteemiarenduse projektide, projekti arendusrühmade, arvutuskeskuse käituse, operatsioonisüsteemide turbe, võrkude, andmebaaside ja rakendussüsteemide, konsultatsioonipunktide, telefonisüsteemide, äritegevuse jätkusuutlikkuse ja avariijärgse taaste valmiduse, IS dokumentatsiooni, elektroonilise andmevahetuse, veebiserveri halduse ja IT halduse puhul.

2.6.2 CRSA-d saab kasutada riskide ja juhtimismeetmete piiritlemiseks ja hindamiseks sihtalal või -talituses ning kõikehõlmava riskihalduse tegevusplaani väljatöötamiseks.

2.6.3 Alternatiivina või lisaks tegevusplaani koostamisele saab CRSA-d kasutada riskialade ja täiendavat kontrollimist vajavate küsimuste esiletõstuks. Täiendava kontrollimise võib sooritada traditsiooniliste IS auditi meetoditega või allutada selle CRSA järeltoimingutele.

2.6.4 CRSA võib osutuda väärtuslikuks suurte projektide plaanimise abivahendiks, sest ta aitab varakult tuvastada ja hinnata riske ning koostada riskihalduse tegevusplaane.

2.7 CRSA omandus

2.7.1 CRSA-s osalejad on protsesside omanikud, st juhtkond ja personal, kes on otseselt seotud vaatlusaluste süsteemide ja küsimustega või keda need mõjutavad, kes seega tunnevad neid kõige paremini ja on sobivate protsessimeetmete rakendamise seisukohalt väga olulised. CRSA tõstab esile tõsiasja, et toimiva ja pideva riskihalduse ja sisejuhtimise eest vastutavad juhid ja personal organisatsiooni kõigil tasemetel.

2.8 CRSA meetodid

2.8.1 CRSA esmased vormid on abistajaga seminarid (tööseminar, *workshop*) ning struktureeritud küsimustikud või küsitlused. Organisatsioonid võivad kombineerida mitut meetodit.

2.8.2 Sageli eelistatakse abistajaga seminare ja need on võimas vahend eeskujulike tulemuste saamiseks lühikese ajaga.

2.8.3 Küsitlusmeetodit või küsimustikku kasutatakse sageli siis, kui soovitud vastajaid on seminarile kogumiseks liiga palju või nad on laialt hajutatud. Neid meetodeid eelistatakse ka siis, kui organisatsiooni kultuur võib pärssida avameelseid arutelusid seminari tingimustes või kui juhtkond soovib minimeerida teabe kogumisega kaasnevat algset aja- ja rahakulu. Isehindamise küsimustikud võidakse luua abistajaga seminaride tulemitena, eesmärgiga kasutada neid seminari kokkulepitud tulemite järeltoimingute vahendina või juhtkonna abivahendina pidevaks toimivate sisemeetmete käigushoiuks ja seireks.

2.9 Alade valimine ja juhtkonna poolehoid

2.9.1 CRSA-d saab rakendada organisatsiooni mitmesugustel tasemetel. Strateegilisel tasemel võivad kõrgem juhtkond ja juhatus kaalutleda riske ja meetmeid, mis mõjutavad üleorganisatsiooniliste eesmärkide saavutamist. Analoogiliselt võivad organisatsiooni allüksused ja talitused tuvastada riske ja hinnata juhtimismeetmeid omaenda sihtide ja tulemite seisukohalt. Allüksuse või talituse valimisel juhindutakse

põhimõttest, et kõnealuse rühma jaoks saab määratleda eesmärkide või tulemite kogumi. See on tähtis, sest rühmas peab valitsema üksmeel selle suhtes, mida on rühmal vaja saavutada, nii et selle põhjal saab kaalutleda ja hinnata riske ja juhtimismeetmeid.

2.9.2 Nagu iga muugi suurema ürituse puhul, on CRSA õnnestumiseks oluline juhtkonna poolehoid ja pühendumus. Kõrgema juhtkonna huvi ja osalus tõendavad organisatsiooni kohustumust integreerida riskihaldus ja juhtimise hindamine organisatsiooni äritegevuse korraldusega kõigil tasemetel. Sellist kohustumust võib kõrgem juhtkond tõendada poliitika või direktiivi andmisega CRSA rakendamise kohta või isikliku teavitamisega CRSA seminaridel.

3 CRSA SEMINAR

3.1 Soovitatavad protseduurid

3.1.1 CRSA eesmärk on anda allüksustele teadmised, oskused ja toetus nende endi riskide kaalutlemiseks ja seireks. See protsess võib aidata IS audiitoril arendada tugevat juhtimiskeskkonda organisatsiooni aladel ning õhutada partnerlikku lähenemist riskihaldusele. Ta võimaldab IS audiitoril anda ettenägelikke ja väärtust lisavaid teenuseid majandusüksuste abistamiseks nende üksuste eesmärkide saavutamise ja seega ka organisatsiooni sihtide saavutamise korraldamisel.

	Soovitatavad protseduurid	√
CRSA seminari plaanimine	Kehtestada seminarile selged eesmärgid ning määratleda organisatsiooniga seotud käsitlusala ja oodatavad tulemid. CRSA eduka seminari läbiviimiseks on väga oluline adekvaatselt plaanida. See võimaldab IS audiitoril formuleerida seminarile sobiva strateegia ja plaani. Seminari valitud meetod võib kõige sobivama vahendina süsteemi riskide ja juhtimismeetmete piiritlemiseks kasutada üht alljärgnevatest alguspunktidest. Iga meetod on kavandatud jõudma samade tulemiteni ning ükski neist ei ole olemuslikult eelistatav. Ärieesmärgid. Seminar keskendub parimale ärieesmärgi saavutamise viisile. Harilikult piiritleb seminar ärieesmärgid, siis tuvastab eesmärki saavutada aitavad hetkel olemasolevad juhtimismeetmed ning seejärel kaalutleb jääkriskid, mida võiks eesmärkide saavutamiseks leevendada. Äririskid. Seminar keskendub eeskätt kõigi äritegevusele või süsteemile toimivate riskide tuvastamisele, sageli toetudes mingile riskide või riskiliikide üldisele meelespeale. Kui seminar on loetlenud kõik võimalikud takistused, ohud või paljangud, uurib ta olemasolevaid juhtimisprotseduure otsustamaks, kas need on kesksete riskide käsitluseks piisavad. Riskid, mida ei ole piisavalt leevendatud, eskaleeritakse ülespoole. Sisemeetmed. Algul keskendub seminar olemasolevate juhtimismeetmete tuvastusele, seejärel aga hindab seda, kui hästi need töötavad riski leevendamiseks ja aitavad saavutada ärieesmärke. Seminar selgitab analüüsimiseks välja lünga meetmete tegeliku toime ja juhtkonna poolt eeldatava toime vahel. Äriprotsessid. Seminar alustab kesksete protsesside uurimisest, hinnates seda, kas iga protsess või alamprotsess annab asjakohaseid tulemusi. Kui tulemusi loetakse vastuvõtmatuiks või ebaadekvaatseteks, analüüsitakse põhjuste tuvastamiseks juhtimismeetmeid.	

Protseduur P5. Juhtimisriski isehindamine (jätkub)

CRSA seminari plaanimine (jätkub)	Määratakse hinnanguliselt seminari lõpukuupäev ja aruandluse ajakava.	
	Hangitakse ja vaadatakse läbi teave seminari käsitlusala ja lahendamisele kuuluvate küsimuste kohta. IS audiitor peaks tutvuma protsesside, tegevuste, riskide, juhtimismeetmete ja seminaril rõhutatavate aladega. Hankimisega võidakse hõlmata järgmine teave: asjassepuutuvad poliitikad, plaanid, õigusaktid, eeskirjad ja lepingud, organisatsiooniteave, rahandusteave, eelmiste auditite tulemid, tegevusala parimad tavad, vaatlusalust ala mõjutavate probleemide üksikasjad ning võimaluse korral ka tulevikus eeldatavalt tekkida võivate jõuproovide ja soodsate võimaluste üksikasjad.	
	Otsustatakse, kuidas, millal ja kellele teatatakse seminari tulemused.	
Osalejate valimine	Seminaril osalejateks valitakse kesksete protsesside omanikud ja protsessis osalev personal. IS audiitor peaks seminari eesmärkide ja käsitlusala põhjal ja eelnevalt kogutud teabe põhjal piiritlema allüksused või talitused, mis peaksid seminaril osalema. IS audiitor võib sõltuvalt organisatsiooni kuuluvate inimeste teadmistest soovitada teatud inimeste osalemist seminaril.	
	Sageli on soovitatav kutsuda seminarile muid keskseid huvipooli, näiteks allüksuse või protsessi olulisi kliente või tarnijaid.	
Seminari ette-valmistamine	Juhtkonna sobivatele tasemetele edastatakse teave osalevate allüksuste või talituste ja osaleva personali kohta. IS audiitor peaks saama mõistliku kinnituse sellele, et osalejad ja asjakohased juhtkonna tasemed tunnevad CRSA protsessi ning teavad selle protsessi võimalikke hüvesid ja väärtust ja pühenduvad neile.	
	Määratakse riski kaalutlemise või hääletamise kogu kasutuselevõetav tehnoloogia ning määratletakse kõigi vastuolude või lahkarvamuste lahendamise mehhanism ja CRSA tulemuste järelkäsitluseks rakendatav lähenemisviis.	
	Eraldatakse seminari jaoks ruumid ning hangitakse instrumendid ja tehnoloogia.	
Seminari instrumendid	Otsustatakse, kuidas tuleb protokollida ja seirata seminari käigus tehtud hindamisi ja otsuseid ning plaanitud toiminguid. Protokollimise ja seire instrumentideks võivad olla lihtsalt paberdokumendid, kuid võidakse kasutada ka riskihalduse tarkvara. Selline tarkvara võib hõlbustada küsitlemist, võib hoida suuri teabekoguseid ja võib aidata ühendada kogu organisatsiooni ulatuses saadud asjassepuutuvat riskiteavet. Ta hõlbustab ka huviobjektide jälitust ja seiret tegevusplaanide elluviimisel. Nagu iga muugi tarkvara, toob ta kaasa kulutusi, mis sisaldavad ta kasutamise litsentsitasu; on ka võimalik, et valmistarkvara funktsioonid ei vasta täielikult ärinõuetele. Hääletamise tehnoloogiat võib kasutada riskihalduse tarkvaraga või eraldi. Teabe ja seisukohtade vaba vahetuse hõlbustamiseks seminaride ajal ning eri seisukohtade ja huvigruppide lahknevuste läbirääkimise abistamiseks võib kasutada anonüümse hääletuse meetodeid.	

Protseduur P5. Juhtimisriski isehindamine (jätkub)

Seminari instrumendid (jätkub)	Lepitakse kokku ühine keel, st sõnavara ja riskiterminite seletussõnastik, mis loob allüksustele ühtse arusaamise.	
	Koostatakse riskide meelespead, st kaalutlemiskriteeriumid ja indikaatorid uute riskide tuvastamiseks või seniste taaskaalutlemiseks. Need meelespead võivad tuua näiteid olukordadest ja sündmustest, mille puhul tuleb allüksuse riskiprofiilid võib-olla uuesti üle vaadata ja ajakohastada.	
Protsessipõhist metoodikat kasutav abistajaga seminar Abistajaga seminar on toimiv vahend allüksuste tutvustuseks CRSA-le, algsete riski kaalutlemiste ja juhtimismeetmete hindamiste sooritamiseks ning äritavadesse integreeritavate instrumentide ja oskuste edastuseks. Siin visandatakse üks soovitatav protsessipõhist metoodikat kasutava seminari vorm.	Saavutatakse ühine arusaam ja kokkulepe selle kohta, millised eesmärgid ja tulemused tuleb saavutada. Ärieesmärgid või allüksuse tulemused moodustavad konteksti, mille taustal kaalutletakse riski ja hinnatakse juhtimismeetmeid. Üks osa sellest protsessist on ka allüksuse eesmärkide sidumine kogu organisatsiooni eesmärkidega. See annab allüksusele strateegilise konteksti ja tõstab töötajate teadlikkust sellest, kuidas nad annavad oma panuse organisatsiooni edusse.	
	Allüksuse eesmärkidele antakse prioriteedid, mis aitavad suunata seminari arutelu kõige olulisematele riskidele ja juhtimismeetmetele ning loovad riskide hindamisele strateegilise konteksti. Toetuda võib näiteks Austraalia riskihalduse standardile (AS/NZS 4360).	
	Kesksete ärieesmärkide alusel tuvastatakse ja kaalutletakse riskid. See tähendab iga riski tõenäosuse ja tagajärgede mõõtude kaalutlemist ning talle üldise riskihinde andmist. Riskihinnet saab kasutada kõige olulisematele riskidele prioriteetide määramiseks. Selle protsessi hõlbustamiseks on kasulik riskiallikate üldistatud meelespea, mis stimuleerib tuvastama, millised riskid võivad toimida konkreetsetele ärieesmärkidele. Need allikad ulatuvad majanduslikest tingimustest juhtkonna tegevuste ja juhtimiseni. Toimealade näiteid on varade ja ressursside baas, tulu ja hüved, inimesed, tegevuste ajastus ja ajakavad. IS projektiga seotud riskid on loetletud lisas 1. Rühm peab kokku leppima tõenäosuse, tagajärgede ja riskihinnete määratluste suhtes.	
	Uuritakse senist juhtimise raamstruktuuri iga tuvastatud riski seisukohalt. Üks kasulik vahend selle protsessi sooritamiseks on juhtimismudel. Need mudelid visandavad mitmesugust tüüpi kasutadaolevaid riski käsitlemise meetmeid, näiteks vastavusmeetmeid, järelevalve meetmeid ja plaanimismeetmeid. Seminarigrupp võib kõik need tüübid ükshaaval läbi vaadata ja teha kindlaks, kas nad on olemas ja kas nad toimivad riski käsitlemisel.	
	Kaalutletakse riskitasemed, mis jäävad alles pärast olemasolevate meetmete rakendamist. Tuleb tuvastada ka asjakohased riskiomanikud, kelle kohus on hallata spetsiifilisi riske. Riskiomanike kohus on otsustada, kas jääkriski tase on aktsepteeritav või on vajalik riski lisakäsitlus.	
	Koostatakse strateegiad ja ajakavad nende riskide käsitluseks, mille tase ei ole aktsepteeritav. Riskiomanike kohus on töötada välja tegevusplaanid.	

Seminari tulemuste valideerimine	Uuritakse ja hinnatakse CRSA seminariga saadud teavet valiidsuse ja nõuetekohasuse aspektist. Millises ulatuses tuleb IS audiitoril sõltumatult valideerida juhtimismeetmeid, oleneb jääkriski tasemest, probleemi tähtsusest, osalejate vaheliste tõenduste kooskõlast ja kogu muust seminariga saadud abiteabest, samuti IS audiitori kutsealasest otsustusvõimest. Meetmete valideerimisele peaks IS audiitor pöörama tähelepanu eriti seal, kus seminar on muundanud suured olemuslikud riskid väikesteks jääkriskideks.	
	Valideerimine võib hõlmata ka küsitlusi järeltoimingutena ja auditi asitõendite kogumist. IS audiitor peaks arutama leebete meetmete hindamist juhtkonna asjakohase tasemega, et saada väärtuslikku tagasisidet paremaks ärieesmärkide saavutamiseks.	
Seminari aruandlus	Iga CRSA üritus peaks väljastama aruande. Üldiselt luuakse aruande sisu arutelude käigus, asjakohaste riskide, juhtimise nõrkuste ja pakutavate parandusmeetmete loetlemise ja kirjeldamise teel. Protokollitakse mitmesugustes arutatud küsimustes saavutatud rühmakonsensus ning enne istungjärgu lõppu vaatab rühm pakutava lõpparuande läbi.	
	Üks CRSA seminari tulemeid on parandusmeetmete plaan, mille vorm sõltub kasutaja nõuetest. IS audiitor peaks andma välja ka formaalse aruande CRSA protsessi ja tulemite kohta, esitades asjassepuutuva tausta, konteksti, riskihinded ja muu materjali vastavalt ISACA IS auditeerimise standardile S7 "Aruandlus".	
Pidev seire	CRSA tähtis osa on see, et allüksused või protsessiomanikud peavad regulaarselt pöörduma tagasi oma riskikaalutluste juurde ja seirama tegevusplaanide elluviimist. Abivahendeiks võivad seejuures olla CRSA pakutavad instrumendid. Kaaluda võib ka järelseminare ning võrgunõupidamised allüksuste esindajatega riskihalduse küsimuste ja probleemide arutamiseks.	
	Seiratakse kokkulepitud toimingute sooritamist, vastavalt harilikele auditeerimise ja tagamise tavadele ning vastavalt ISACA IS auditeerimise standardile S8 "Järeltoimingud".	

4 JÕUSTUMISKUUPÄEV

4.1 See protseduur kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. augustil 2003 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

LISA

Toetumine COBITile

Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ja arvestades COBITi teabekriteeriume.

COBIT annab infosüsteemide keskkonna tarbeks detailse juhtimismeetmete ja juhtimismeetodite kogumi. Seire alal on COBITil lai juhtimiseesmärk "Hinnata sisejuhtimise adekvaatsust" (S2), mille taga on rida detailseid juhtimiseesmärke, näiteks sisejuhtimise seire, õigeaegne sisemeetmete rakendamine ja sisejuhtimise

Protseduur P5. Juhtimisriski isehindamine (jätkub)

aruandlus. Iga sellise detailse juhtimiseesmärgi saavutamisele saab kaasa aidata juhtimisriski isehindamise meetodite kasutamine. Juhtimisriski isehindamise meetodeid saab kasutada nii selliste detailsete juhtimiseesmärkide saavutamise ulatuse hindamiseks mingil alal või mingis talituses kui ka selle ala või talituse abistamiseks ta soorituse parandamiseks nende eesmärkide saavutamisel.

Plaanimise ja organiseerimise alal on COBITil lai juhtimiseesmärk "Kaalutleda riskid" (PO9), mille taga on rida detailseid juhtimiseesmärke, näiteks riskide tuvastamine, riskide mõõtmine ja riskimeetmete plaan. Ka iga sellise detailse juhtimiseesmärgi saavutamisele saab kaasa aidata juhtimisriski isehindamise meetodite kasutamine. Juhtimisriski isehindamise meetodeid saab kasutada olemuslike ja jääkriskide tuvastamiseks ja kaalutlemiseks mingil alal või mingis talituses ning abivahendina nende riskide toimiva haldamise tegevusplaani väljatöötamisel.

IT-projektiga seotud riskide näide

- **Ärialased**
  - Projekti- või süsteeminõuded pole adekvaatselt määratletud
  - Projekti- või süsteeminõuete muudatustega ei tulda toime
  - Projekti tulemid ei rahulda ärivajadusi
  - Projekti tulemite ajastus ei rahulda ärivajadusi
  - Vajalike ärialaste muudatustega ei tulda toime
- **Allettevõtu alased**
  - Hinnamuutused
  - Allettevõtjal puuduvad ressursid, kui neid on vaja
  - Toode või teenus ei vasta ootustele
  - Allettevõtja ei tule toime
  - Allettevõtu tingimuste täitmist ei saa sundida
- **Välised**
  - Uute tehnoloogiate ilmumine
  - Kesksete tehnoloogiate tõrge
  - Oluliste teenuste (näiteks side või energiatoite) tõrge
  - Tarnija või muu sisendressursside andja vahetumine või väljalangemine
  - Organisatsiooni ülevõtmine
- **Rahalised**
  - Rahastamine muutub osaliselt või täielikult kättesaamatuks
  - Projekti eelarve osutub ebatäpseks
  - Suureneb oluliste sisendressursside maksumus
  - Ei tulda toime lepinguhälvetega
  - Projekti eelarve ületatakse

Protseduur P5. Juhtimisriski isehindamine (jätkub)

- **Teostusalased**
  - Omavahel seotud projektid nurjuvad või hilinevad
  - Halb projektihalduse metoodika
  - Halb süsteemiarenduse metoodika
  - Halvasti toimiv projektiaruandlus
  - Projekti ei lõpetata õigeks ajaks
- **Tulemialased**
  - Eeldatud ärialased hüved projekti teostamisest ei realiseeru
  - Süsteemide halb dokumentatsioon
  - Teostusjärgsed probleemid ja kulud
  - Süsteemi hoolduse probleemid ja kulud pikemas perspektiivis
- **Ressursialased**
  - Oskused on teostamise edukaks lõpetamiseks puudulikud
  - Kvalifitseeritud inimressursid ei ole kättesaadavad
  - Kvalifitseeritud inimressursse ei säilitata
  - Riistvara ei ole nõuetekohaselt käideldav
- **Strateegilised**
  - Projekti tulemid ei ole kooskõlas organisatsiooni eesmärkide ja prioriteetidega
  - Organisatsiooni prioriteetide või suuna muutus
  - Projekti käsitlusala laienemine
- **Süsteemi integratsiooni alased**
  - Platvorm ei sobi
  - Projektiga seotud senised süsteemid, protsessid või riistvara ei ühildu projektiga
- **Tehnoloogilised**

- Projekti sisendressursid ei toimi ootuspäraselt
- Projekti tulemid ei toimi ootuspäraselt

Protseduur P6. Tulemüürid

1. TAUST

1.1 Seosed standarditega

1.1.1 Standard S6 „Audititöö sooritamine“ määrab: “IS auditi meeskonna üle peaks teostama järelevalvet, et anda mõistlik kinnitus auditi eesmärkide saavutamise ja kohaldatavate professionaalsete auditistandardite täitmise kohta.“

1.1.2 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.3 Suuniseid annab suunis G25 „Virtuaalsete privaatvõrkude läbivaatus“.

1.1.4 Suuniseid annab protseduur P3 „Sissetungi tuvastamise süsteemide (IDS) läbivaatus“.

1.2 Seosed COBITiga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

• sooituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?

• IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?

• teadlikkusele: millised on eesmärkide saavutamata jätmise riskid?

• mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed soorituse indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

1.3 Protseduuri vajadus

1.3.1 See dokument on esmajärjekorras mõeldud IS sise- ja välisaudiitoritele, aga teda saavad kasutada ka teised IS turbe asjatundjad, kelle vastutada on tulemüüri konfiguratsioon.

1.3.2 Tänapäevased ettevõtted on organiseeritud hulga tuumikprotsessidena, mis töötavad nõudluse ja pakkumise võrkudes. Peaaegu iga organisatsioon maailmas seisab vastakuti kasvava vajadusega toimivuse ja tõhususe järele (s.t kõrgemad kvaliteedinõuded toodetele ja teenustele, käibe kasvatamine, kulude vähendamine, uute toodete väljaarendamine); see on vajadus paremate, kiiremate ja odavamate protsesside järele. Neid üha keerukamaid töövõrke toetavad kättesaadavad sidetehnoloogiad (peamiselt Internet), mis võimaldavad ettevõtetel keskenduda tuumikpädevustele ja teha teistega koostööd klientidele lisaväärtuse pakkumiseks.

1.3.3 Uued sidekanalid teevad võimalikuks vanade protsesside ümberkujundamise. Need kanalid pakuvad uusi võimalusi mitmesuguste süsteemide ja võrkude ühendamiseks, tehes nad kättesaadavaks rohkematele inimestele ning võimaldades olemitel ja nende protsessidel interakteeruda (nt e-hangete ja e-väljatöötuse puhul).

1.3.4 Need uued protsessid on osutanud vajadusele uute meetodite järele, mis lubaksid volitatud juurdepääsu organisatsiooni andmetele ja programmidele ning kaitseksid neid andmeid ja programme volitamata (ja üldjuhul pahatahtliku) juurdepääsu eest uute kanalite kaudu, mis ühendavad seniseid võrke väliste allikatega. Seda arvestades on välja töötatud erifunktsionaalsusega seadmed (tulemüürid), mis aitavad leevendada nimetatud riske.

1.3.5 Tulemüüre on mitut liiki ning neid kasutatakse paljudes erinevates konfiguratsioonides, millest igaüks on mõeldud rahuldama spetsiifilist kaitsevajadust.

1.3.6 See dokument annab mõned suunised IS audiitoritele, kellel tuleb üha enam auditeerida või läbi vaadata uusi protsesse, mis ühendavad omavahel erinevaid olemeid Interneti, otseühenduste või rendivõrkude vahendusel. Seetõttu peavad IS audiitorid hindama turvabarjääride tugevust, et saada mõistlik kinnitus teabe tervikluse, käideldavuse ja konfidentsiaalsuse kohta.

Protseduur P6. Tulemüürid (jätkub)

2. TULEMÜÜRID

2.1 Tulemüüride liigitus

Märkus: Akronüüm OSI tähistab avatud süsteemide sidumise arhitektuuri (*Open Systems Interconnection*).

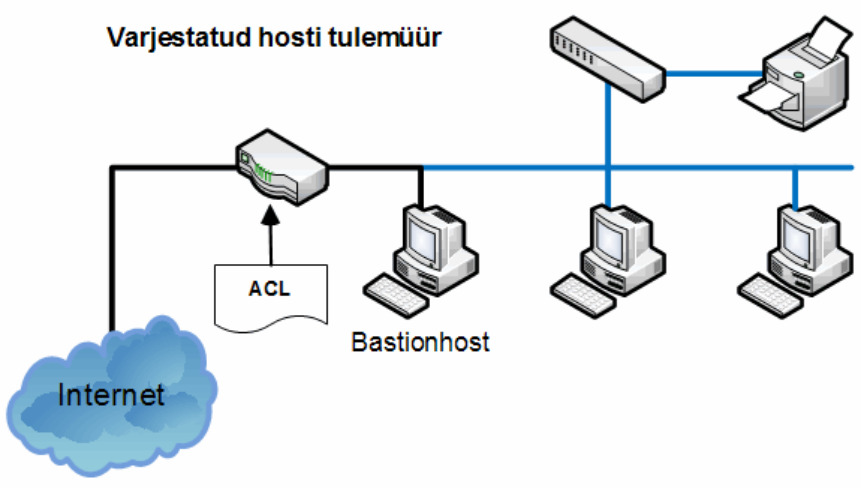
OSI kiht/ tulemüüri liik	7 Rakendus-	6 Esitus-	5 Seansi-	4 Transpordi-	3 Võrgu-	2 Andmelüli-	1 Füüsiline
Ruutereid kasutatakse tulemüürina							
Paketifilter				(mitte alati toetatud)			
Olekufilter							
Hübriidsed tulemüüri-tehnoloogiad							
Rakendusproksi lüüs				(hõlmatud kihi 7 funkt-sioonide tulemusel)			

2.1.1 Üldiselt teevad võrgukihi tulemüürid otsuseid, arvestades lähtepunkti, sihtaadresse ja eraldiseisvaid IP-pakette. Üks lihtne marsruuter on näiteks "harilik" võrgukihi tulemüür, sest ta ei suuda vastu võtta kuigivõrd keerulisi otsuseid selle kohta, kuhu on pakett tegelikult suunatud või kust see tegelikult tuli. Tänapäevased võrgukihi tulemüürid on muutunud üha keerukamaks ja talletavad sisemiselt teavet neid läbivate ühenduste olekute kohta, teatud andmevoogude sisu kohta jne. Oluline erinevus paljude võrgukihi tulemüüride puhul on see, et nad marsruudivad liiklust otse läbi eneste, seega tuleb mõne sellise kasutamiseks kas vallata avalikku IP-aadressiplokki või kasutada "privaatse Interneti" aadressiplokki. Võrgukihi tulemüürid on tavaliselt väga kiired ning kasutajatele väga läbipaistvad.

2.1.2 Varjestatud hosti tulemüürid kontrollivad juurdepääsu ühele hostile ja väljapääsu sealt, kasutades võrgukihis töötavat marsruuterit. Üksikhost on harilikult bastionhost – hoolikalt kaitstud ja turvatud tugipunkt, mis suudab vastu seista rünnetele.

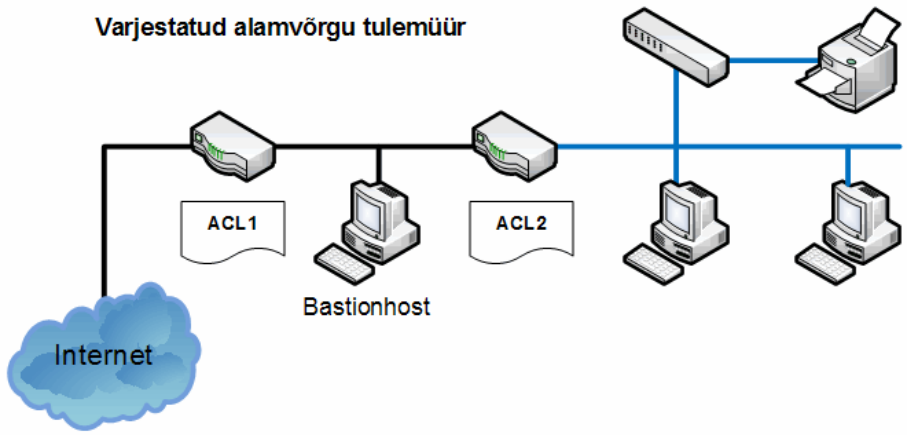
Internet	Väline marsruuter	Bastionhost	Sisevõrk	Usaldatud seadmed
liiklus →	liiklus →←	liiklus →←	liiklus →←	liiklus ←

Protseduur P6. Tulemüürid (jätkub)



2.1.3 Varjestatud alamvõrgu tulemüürid kontrollivad juurdepääsu kogu võrgule ja väljapääsu sealt, kasutades võrgukihis töötavat marsruuterit. See on sarnane varjestatud hostile, selle vahega, et tegelikult on see varjestatud hostide võrk.

Internet	Väline marsruuter	Bastionhost	Perimeetervõrk	Sisemine marsruuter	Sisevõrk	Usaldatud seadmed
liiklus →	liiklus →←	liiklus →←		liiklus →←	liiklus →←	liiklus ←



2.1.4 Paketifilter-tulemüürid (perimeeterlahendused) analüüsivad kõiki nendeni jõudvaid pakette, seejärel edastavad või viskavad need ära vastavalt määratud reeglitele. Pakettide filtreerimine kasutab liiklusvoo piiramiseks paketi päisest võetud teavet lähte- või sihtpunkti, protokolli ja portide kohta. Paketifilter-tulemüürid on võib-olla kõige enam levinud, ning neid on kõige lihtsam kasutusse võtta väikestes lihtsates saitides. Paraku kannatavad sellised tulemüürid mitmete puuduste all ning on seetõttu vähem soovitud kui teised tulemüürid.

Protseduur P6. Tulemüürid (jätkub)

Pakette filtreeriv marsruuter paigaldatakse Interneti (või suvalise alamvõrgu) lüüsi juurde, misjärel seadistatakse marsruuteris pakettide filtreerimise reeglid, millega blokeerida või filtreerida protokolle ja aadresse. Saidi süsteemidel on tavaliselt otsepääs Internetti, samas kui pääs Internetist saidi süsteemidele on täielikult või põhiosas blokeeritud. Samas võib marsruuter poliitikast sõltuvalt lubada valikulist juurdepääsu süsteemidele ja teenustele. Loomuomaselt ohtlikud teenused nagu NIS, NFX ja X-Windows on tavaliselt blokeeritud.

Paketifilter-tulemüüre võib leida TCP/IP-põhistest võrkudest, aga ka teistest võrgukihi adresseeringut (näiteks IPX) kasutavatest võrkudest. Mõned marsruuterid saavad pakkuda algelisi funktsioone transpordikihi vahendusel, niiviisi realiseerides olekufiltriga lihtsa tulemüüri. Kuna kasutatavad filtreerimisreeglid on väga lihtsad, võimaldab see suurt töötlemiskiirust, kuid muudab samas tulemüüri aldiks väärale häälestusele, kui määratletakse reeglite kogum, mis ei vasta organisatsiooni turvapoliitikale.

Kuna sellised tulemüürid ei analüüsi kõrgemaid andmekihte, ei sobi nad kaitseks rünnete eest, mis sooritatakse rakenduse funktsioonide abil; ka ei paku nad toimivat kaitset spuufimisrünnete eest. Ka on neil piiratud logimisvõime. Selliseid tulemüüre kasutatakse keskkondades, mis nõuavad suurt töötluskiirust, kuid mitte keerulisi logimis- või autentimisfunktsioone. Sellise funktsionaalsuse saab lisada ainsa tulemüürivahendina (näiteks marsruuterisse), aga see võib olla ka üks teiste, kõrgemates kihtides töötavate seas.

Internet	Tulemüür	Sisevõrk	Usaldatud seadmed
liiklus →	liiklus →←	liiklus →←	liiklus ←

2.1.5 Oleku filtreerimine (ehk dünaamiline pakettide filtreerimine) (*stateful inspection / dynamic packet filtering*, SI/DPF) on tulemüüriarhitektuur, mis töötab võrgukihis. Erinevalt staatilisest pakettide filtreerimisest, mis analüüsib paketi päises olevat teavet, analüüsib oleku jälgimine lisaks paketi päisele ka paketi sisu, et selgitada välja rohkemat paketi kohta kui vaid teavet tema lähte- ja sihtpunkti kohta. See meetod kasutab kombinatsiooni pakettide filtreerimisest, oleku jälgimisest ja proksidest.

SI/DPF kasutab olekutabeleid ja programmeeritud juhiseid, et analüüsida teavet, mis pärineb paketi päisest ja paketi sisust (rakenduse olek) kuni rakenduskihini välja. Teave töödeldakse ja talletatakse, et anda tulemüürile kontekst, mille järgi klassifitseerida liiklust.

Peamine eesmärk on teha kindlaks paketid, mis kuuluvad algatatud ühendusse ning avada ja sulgeda spetsiifilisi porte selle liikluse jaoks. Olekufiltriga tulemüür seirab ka ühenduse olekut ja koostab teabe põhjal olekutabeli.

Need seadmed analüüsivad pakette, jättes meelde, millised ühendused kasutavad milliseid pordinumbreid ning sulgevad pääsu nendele portidele, kui ühendus sulgub. Avaldised, millega defineeritakse filtrid, tuleb kirjutada tootja süntaksi järgi. SI/DPF laiendab tulemüüri operatsioonisüsteemi, säilitades rakenduse oleku ja paketipäise

teabe tabelis. Seda tabelit kasutatakse, et klassifitseerida liiklust ja rakendada erinevaid töötlemisreegleid algatatud ühendustele ning hallata spetsiifiliste portide avamist ja sulgemist.

2.1.6 Hübriidtulemüürid kombineerivad pakettide filtreerimise ja rakendustaseme filtreerimise omadused. Hübriidtulemüürid, nagu ka paketifilter-tulemüürid, töötavad OSI mudeli võrgukihis, filtreerides kõiki sissetulevaid pakette lähte- ja sihtkoha IP-aadresside ja pordinumbrite alusel ning tehes kindlaks, kas seansipaketid on asjakohased. Nad suudavad töötada ka rakendustaseme tulemüüridena, s.t nad suudavad läbi vaadata iga paketi sisu kuni rakenduskihini välja. Tavaliselt kasutavad nad mõnda paketi- ja rakenduse filtriga toote turvaomaduste kombinatsiooni. Hübriidtulemüür kasutab kombinatsiooni pakettide filtreerimisest, oleku jälgimisest ja proksidest. Eesmärk on töödelda mitmesugust tüüpi andmeliiklust vastavalt ohule, mida see endast kujutab, ning leida tasakaal läbilaske ja töötlusaja vahel. Hübriidteostuse puhul on osad hostid hariliku tulemüüri taga, ülejäänud väljaspool seda. Kesksaidis asuv IPSec-lüüs tagab ühenduse väljaspool asuvatele masinatele. Selline seadistus on levinud organisatsioonides, kus on suur kesksait ja teatud arv kaugtöötajaid. Nagu tavalises virtuaalses privaatvõrgus (VPN), on kaughostidel IPSec-tunneli kaudu täielik juurdepääs sisevõrgule. Sarnaselt on kaitstud liiklus sisemasinatest kaugsõlmedesse. Erinev on, et liiklust kaugsõlmedest ülejäänud Internetti reguleerib kesksaidi turvapoliitika, s.t tulemüüri ülem levitab turvapoliitika kaugsõlmedeni. Ideaaljuhul kasutatakse sama poliitikalausungit ka hariliku tulemüüri ohjamiseks, tagades niiviisi ühtse turvapoliitika.

2.1.7 Proksi-tulemüürid käitavad eritarkvara, mis lubab töötada spetsiifilistel programmidel ning kehtestada autentimise, filtreerimise ja logimise poliitikaid. Näiteks HTTP-proksi on kirjutatud spetsiaalselt selleks, et lubada ainult ja üksnes HTTP-pääs läbi enda. Ka nõuab see kasutajalt eritoiminguid (näiteks peab kasutaja brauseris käsitsi tegema asjakohased sissekanded prokside kohta). Kuna neil pole tulemüüri võimet, tuleb nad paigutada tulemüüri taha. Kasutaja, kes vajab juurdepääsu välistele ressurssidele, peaks kasutama proksit, mis suudab tagada kasutaja autentimise, logida kasutaja tegevusi ja läbi vaadata näiteks veebi ja e-maili sisu. Täiendavad toetatud funktsioonid on näiteks sisu läbivaatus, teenuste blokeerimine, viiruste eemaldamine jne. Tüüpiliselt käituvad proksi-tulemüürid kasutaja päringute vahendajana – nad loovad teise ühenduse soovitud ressursiga kas rakenduskihis rakendusproksi vahendusel või sessiooni- või transpordikihis virtuaalse kanali vahendusel. Neid läbivad kõik võrku sisenevad ja sealt väljuvad sõnumid. Tulemüür lubab proksiga suhelda ainult välistel süsteemidel. Sisuliselt varjab proksi tegelikud võrguaadressid.

Väline host	Internet	Tulemüür	Sihtotstarbeline proksi	Sisevõrk	Usaldatud seadmed
liiklus →	liiklus →	liiklus →←	liiklus →←	liiklus →←	liiklus←

Protseduur P6. Tulemüürid (jätkub)

Proksi-tulemüüride eelised:

• Proksi on tavaliselt väga teadlik käsitletavast andmevormingust, oskab tuvastada ebakõlasid ning pakkuda nende eest kaitset.

• Lubada tuleb ainult teatud toetatavad protokollid.

Proksi-tulemüüride puudused:

• Iga uue protokolli lubamiseks on vajalik proksi, mis on teadlik just sellest protokollist.

• Kui olemasolevat protokolli laiendatakse, vajab proksi tarkvara ilmselt uuendamist.

Proksi-tulemüür loob sisemiste ja välimiste süsteemide vahele kontrollitud võrguühenduse. Proksi ja sisemise kliendi vahel on virtuaalne kanal. Päringud Internetti jõuavad selle kanali kaudu proksini, mis muudab IP-aadressi ja edastab päringud Internetti; väliskasutajad näevad ainult proksi IP-aadressi. Seejärel võtab proksi vastused vastu ja saadab need läbi kanali tagasi kliendile. Kuigi läbiv liiklus on lubatud, ei näe välised süsteemid kunagi sisemisi süsteeme. Sedalaadi ühendust kasutatakse tihti selleks, et ühendada "usaldatud" sisekasutajad Internetiga, kõige sagedamini aga väljuvate ühenduste jaoks, mis vahendavad TCP-ühendusi ja on kasutajale nähtamatud. Saate ajal kopeerivad lüüsi retranslatsiooniprogrammid baite edasi-tagasi ning lüüs toimib kaablina.

Automaatühenduse suutvus abistab, kui näiteks välishostid väljaspool lüüsi vajavad juurdepääsu seespool asuvale printerile. Teostatakse portide määramise ja pääsukontrolli piirangud. Kui välisesse hosti luuakse ava, aitab automaatühendus ühendust ohjata. Käsiteenindus on ühendusteenuse protokoll, mis tuleb teostada, et määratleda soovitav sihtpunkt. Teostatakse kas proksi (sihtpunkti hostinimi) või SOCKS (IP-aadress). Logid talletavad baidid ja TCP sihtpunkti, aga ei vaata neid läbi.

Automaatühendusega proksi-tulemüüride eelised:

• Nad on turvalisemad kui paketitaseme lüüsid, kuigi mitte nii turvalised kui rakenduse lüüsid;

• Taasesitavad TCP-ühendusi;

• Annavad lube pordiaadressi alusel;

• Suudavad aru saada paketi sisust.

Automaatühendusega proksi-tulemüüride puudused:

• Sissetulevad ühendused on loomuomaselt riskantsed. Sellised tulemüürid edastavad pakette ilma ülevaatuseta, neil on piiratud auditisuutlikkus ning neil puuduvad rakendusespetsiifilised meetmed.

• Puudub rakendustaseme kontroll

2.1.8 Läbipaistvad tulemüürid on segu proksi-tulemüüridest ja võrguaadresside transleerimisest (NAT) (vt 4.1.1). Sarnaselt NAT-tulemüüriga peab sisemine masin teadma vaid seda, kuhu saata pakette, et need jõuaksid väljaspoole. Samas võib tulemüür turvaeesmärkidel läbipaistvalt rakendada teatud liiklusele proksisarnaseid mehhanisme, selle asemel, et sellist liiklust pimesi edastada. Sisemistel masinatel võib olla, aga võib ka mitte olla privaatne IP-aadressivahemik.

Protseduur P6. Tulemüürid (jätkub)

Läbipaistvate tulemüüride eelised:

• Ei vaja kliendipoolset erihäälestamist, just nagu ka NAT-tulemüür;

• Võimaldab hästituntud teenuste peenemat kontrolli ja kaitset.

Läbipaistvate tulemüüride puudused:

• Enamik puudusi on samad, mis NAT-tulemüüril. Kui teatud rakendusprotokolli kasutatakse ebastandardses pordis, lähevad kaduma kõik "erilised" kaitsevahendid. Sõltuvalt lubatud reeglitest võib see isegi üldse mitte juhtuda.

2.1.9 Rakendustaseme (lüüsi) tulemüürid sisaldavad kogu sihtotstarbelise proksi funktsionaalsust pluss tulemüüri funktsionaalsust (s.t igal proksirakendusel on juurdepääs tulemüüri reeglite baasile, mille põhjal pakette lubada või keelata).

Harilikult käitavad sellised hostid proksisid, mis ei luba otseliiklust võrkude vahel ja mis sooritavad keerukat läbiva liikluse logimist ja revisjoni, kuna nad saavad üle vaadata kõik paketid (nende sihtaadressid, pordid ja sisu). Nad võivad teostada laiendatud autentimismeetodeid, kuna nad saavad kombineerida rohkem teavet (nad saavad arvesse võtta rohkem teavet kui paketi- ja olekufiltriga tulemüürid, mis autendivad kasutajaid kergestivõltsitava võrgukihi-aadressi alusel). Kuna proksirakendused on tarkvarakomponendid, mis töötavad tulemüüris, on see hea koht ulatuslikuks logimiseks ja pääsukontrolliks. Rakendustaseme tulemüüre saab kasutada võrguaadresside translaatoritena, kuna liiklus siseneb ühest otsast ja väljub teisest, olles läbinud rakenduse, mis toimivalt maskeerib lähteühenduse päritolu. Kui mõni rakendus peaks ette jääma, võib see mõnel juhul mõjutada sooritust ja muuta tulemüüri vähem läbipaistvaks (suure läbilaskega rakenduste kasutamisel eelistatakse tihtipeale lahendust, kus tulemüüri taga asub sihtotstarbeline proksi).

Rakendustaseme tulemüür, mida nimetatakse ka topeltliidesega lüüsiks, on kõrgelt turvatud host, mis käitab proksitarkvara. Tal on kaks võrguliidest (üks mõlemas võrgus) ja ta blokeerib kogu läbiva liikluse.

Internet	Tulemüür (topeltliidesega host)	Sisevõrk	Usaldatud seadmed
liiklus →	liiklus →←	liiklus →←	liiklus ←

Rakendustaseme (lüüsi) tulemüüride eelised:

• Kogu sisenevat ja väljuvat liiklust on kergem logida ja kontrollida;

• Rakendustaseme tulemüürid saavad hõlmata krüpteerimise, et kaitsta andmeedastust.

Rakendustaseme (lüüsi) tulemüüride puudused:

• Töömahukas haldus – iga võrku ühendatud teenus vajab eraldi konfigureerimist (näiteks HTTP, Telnet, e-mail, uudisegrupid);

• Sisekasutajad peavad enamike teenuste jaoks kasutama proksist teadlikke kliente.

• Ilma teenuseklienti täiendavalt modifitseerimata peaks kasutaja ühenduma tulemüüriga. Modifikatsioonide rakendamisel saab selle ühenduse teha kasutajale läbipaistvaks.

3. TULEMÜÜRIDELE ÜHISED TUNNUSED JA FUNKTSIONAALSUS

3.1 Võrguaadresside transleerimine (NAT)

3.1.1 NAT on vahend, millega "varjata" tulemüüri taga kasutatav võrguadresseerimise skeem. See võimaldab tulemüüri taga kehtestada valitud adresseerimisskeemi, säilitades samas suutlikkuse ühenduda väliste ressurssidega läbi tulemüüri. See võimaldab ka mittemarsruuditavate IP-aadresside vastendamist väiksemale hulgale kehtivatele aadressidele. Võrguaadresside transleerimisel on kolm režiimi:

• Staatiline NAT – Iga privaatvõrgu sisemise süsteemiga on seostatud talle vastav väline, marsruuditav IP-aadress. Selle tehnikaga saab säilitada võimaluse anda välistele kasutajatele valikuline juurdepääs (nt võib väline süsteem pöörduda sisemise serveri poole, mispuhul tulemüür sooritaks vastendamise mõlemal, väljuval või siseneval suunal).

• Varjav NAT – Kõik sisemised IP-aadressid on peidetud ühe IP-aadressi taha. Sellise seadistuse peamine nõrkus on, et kord juba tulemüüri taha paigutatud ressursse pole võimalik teha kättesaadavaks välistele kasutajatele, kuna tagurpidine vastendamine väljastpoolt sissepoole pole võimalik. Seetõttu tuleb süsteemidel, mis peavad olema kättesaadavad välistele süsteemidele, jätta aadressid vastendamata. Sedalaadi teostus nõuab, et tulemüür kasutaks enda välisliidese aadressi asendus- või transleeritud aadressina, vähendades konfiguratsiooni paindlikkust.

• Pordiaadressi transleerimine (PAT) – Sarnane varjavale NAT-ile, mõne erinevusega. PAT ei nõua tulemüüri välisliidese IP-aadressi kasutamist ning tulemüüri taga paiknevatele ressurssidele saab juurdepääsu anda valikuliselt, edastades teatud pordinumbritest sisenevad ühendused spetsiifilistele hostidele.

3.1.2 NAT-i eelised:

• Ei nõua kliendilt erikonfigureerimist, välja arvatud tavaline marsruutingu konfigureerimine. Kliendid peavad teadma ainult enda vaikelüüsi.

3.1.3 NAT-i puudused:

• Puudub täiendav turvalisus, mis oleks enamat kui valik "lubada seda tüüpi liiklus". Kui sisemine klient on juba lubatud protokolli kaudu ühendunud, võib juhtuda ükskõik mis, mis jääb selle protokolli piiresse.

• Pole võimalik lubada eriprotokolle, mis nõuavad vastuühenduse tekitamist.

3.1.4 Kui teatud tüüpi protokolle hakatakse piirama, saab juurdepääsu jätta vaid teatud portidele. Ühest küljest on see liiga tõkestav, kuna sisekasutajad ei pruugi saada juurdepääsu ebatüüpseid porte kasutavatele veebiserveritele. Samas on see liiga lubav, kuna välisel ebatüüpsel pordil võib töötada keelatud teenus, millele sisekasutajad saaks sellisel juhul ligipääsu.

3.2 Sissetungi tuvastamise süsteemid (*Intrusion Detection Systems*, IDS)

3.2.1 Need süsteemid on kavandatud, et teavitada ja ära hoida volitamata juurdepääs võrku ühendatud süsteemile või ressursile. Sageli suhtlevad nad tulemüüridega, et avastatud rünnakule järgneks automaatne reageering (nt ründeallika blokeerimine).

3.2.2 Ründetuvastuse ja -reageeringu tarkvara seirab pidevalt võrguliiklust, otsides tuntud ründekäekirju. Kui tarkvara avastab volitamata tegevuse, reageerib ta sellele automaatselt mingi süsteemiülema määratud vastutegevusega.

3.2.3 Nõuded heale sissetungi tuvastamise süsteemile on järgmised.

• Paigaldatav läbi kogu üldise võrgu, et tagada turvalisus kogu ettevõttes;

• Seirab sisenevat ja väljuvat liiklust;

• Pakub kaitset kohtvõrkudele ning Interneti-, intraneti- ja sissehelistamispöördusele;

• Annab reaalajas häiret asjakohasele personalile, näiteks süsteemiülematele ja turvaametnikele;

• On konfigureeritav nii, et sissetungija kõrvaldatakse automaatselt ning blokeeritakse tema järgnev sisenemine;

• Logib valikuliselt seansiandmeid;

• Annab kontrolljälje, mille abil saab ründe taasluua juurdlusejärgse analüüsi jaoks;

• Võimaldab kaughaldust ja suudab haldusseansid turvaeesmärkidel krüpteerida (kui klientorganisatsioon seda nõuab).

3.2.4 Sissetungi tuvastamise süsteemid ei suuda aidata järgmistel juhtudel.

• Võrguprotokollide nõrkuste kompenseerimine;

• Kogu liikluse analüüsimine hõivatud võrgus;

• Mõningase tänapäevase võrguriistvara ja seonduvate vahendite käsitlemine;

• Identifitseerimis- ja autentimismehhanismi(de) nõrkus(t)e kompenseerimine;

• Süsteemi antava teabe kvaliteedi või tervikluse probleemide kompenseerimine;

• Rünnetejärgsete juurdluste läbiviimine ilma inimese sekkumiseta.

Protseduur P6. Tulemüürid (jätkub)

3.2.5. IDS-i paigaldamine peaks algama võrgu perimeetri kehtestamise ja kõikide võimalike sisenemispunktide väljaselgitamisega. Kui sisenemispunktid on välja selgitatud, saab paigaldada IDS-i andurid, mis on konfigureeritud saatma aruandeid kesksele halduskonsoolile. Võimalike paigalduskohtadena soovitatakse järgmiseid.

• Võrgu ja ekstraneti vahel;

• Tulemüüri ees DMZ-s (demilitariseeritud tsoon, vt 5.2), et teha kindlaks ründed DMZ-s asuvate serverite aadressil;

• Tulemüüri ja võrgu vahel, et oht kindlaks teha, kui tulemüürist on läbi tungitud;

• Kaugpöörduse keskkonnas;

• Kui võimalik, siis serverite ja kasutajaskonna vahel, et avastada seestpoolt lähtuvad ründed;

• Intranetis, FTP- ja andmebaasikeskkondades.

3.2.6 Sissetungi tuvastamise süsteemid saab liigitada kaheks: hostipõhised ja võrgupõhised. Võrgupõhine sissetungi tuvastamine on tavaliselt tõhusam kui hostipõhine tuvastamine, kuna on võimalik seirata paljusid süsteeme ja ressursse. Sedatüüpi süsteemid tekitavad harilikult vääraid ründetuvastusi ning vajavad inimsekkumist, et teha kindlaks tegelikud ründed. Need kaks IDS-ide kategooriat on määratletud järgmiselt.

• Hostipõhine sissetungi tuvastamine – See on operatsioonisüsteemiga tihedalt integreeritud ning tuleks paigaldada igasse arvutisüsteemi, mida tahetakse kaitsta. Sellise süsteemi kasutamisel kerkivad üles järgmised probleemid.

− Nad avaldavad süsteemi jõudlusele negatiivset toimet.

− Nad ei paku toimivat avastamist võrreldes võrgupõhistega (nt teenusetõkestusrünne).

− Nad võivad mõjutada süsteemi stabiilsust.

• Võrgupõhine sissetungi tuvastamine – Analüüsib protokolle ja seirab võrguliiklust, otsides spetsiifilisi sõnesid, mis võivad osutada teatud tüüpi rünnakutele. Sellise süsteemi kasutamisel kerkivad üles järgmised probleemid.

− Enamikel juhtudel ei suuda nad toimivalt avastada ründekäekirju, mis on jagatud paljude pakettide vahel.

− Tavaliselt nõuavad nad erilist seadmekonfiguratsiooni (võimalus, mis pole vahel toetatud), et kehtestada võrguliidesel liberaalne režiim.

− Neid saab avastada, tuvastades liberaalses režiimis töötava võrguliidese.

− Mõnikord on raske ennustada, milline käekiri osutab ründele.

Protseduur P6. Tulemüürid (jätkub)

3.3 Virtuaalsed privaatvõrgud (VPN)

3.3.1 Virtuaalne võrk on ehitatud olemasoleva võrgumeedia peale krüpteeritud või krüpteerimata kujul, et tekitada turvalised võrguühendused üle mitteusaldatud võrkude (nt Internet). Seda tehnoloogiat saab kasutada turvalise kaugpöörduse andmiseks ettevõtte võrkudesse või erinevate organisatsioonide võrkude ühendamiseks. Kõige sagedamini kasutatavad protokollid on

• IPSec,

• PPTP (*Microsoft Point-to-Point Tunneling Protocol*),

• L2TP (*Layer 2 Tunneling Protocol*).

4. TULEMÜÜRIDE LEVINUMAD KONFIGURATSIOONID

4.1 Levinumad otstarbed tulemüürikonfiguratsioonidele

4.1.1 Kõige levinumad tulemüüride otstarbed on järgmised.

• Kontrollib pääsu sisemiste ja välimiste võrkude jaoks (perimeetri tulemüürid)

• Kontrollib pääsu avaliku juurdepääsuga ja avaliku juurdepääsuta serverite vahel (DMZ tulemüürid)

• Kontrollib pääsu sisevõrkude vahel, millel on erinevad pääsu- ja turvanõuded

• Kontrollib pääsu läbi modemipuulide ja era-sissehelistamisvõrkude

• Kontrollib pääsu kolmanda osapoole hallatavatesse hostidesse ja võrkudesse ning neist välja

• Krüpteerib sisemisi ja välimisi võrke, mis edastavad tundlikku teavet

• Varjab sisemisi võrguaadresse väliste võrkude eest (NAT)

4.2 Demilitariseeritud tsoon (DMZ)

4.2.1 DMZ suurendab oluliselt võrgu turvalisust, kaitstes iga arvutit, mis peab olema kättesaadav ühe tulemüüri taga asuvast välisvõrgust ning lisades kaitsekihi jagatud masina ja sisevõrgu vahele. Kui DMZ on asjakohaselt seadistatud, peab ründaja rikkuma kaks turvakihti, et jõuda millegi väärtuslikuni.

4.2.2 Selline konfiguratsioon suurendab oluliselt nõudmisi oskustele, mida väline häkker peab valdama sisevõrgu rikkumiseks, ning seega vähendab sisevõrgu rikkumise ohtu. Riski saab veelgi vähendada, kasutades mitmesuguseid ühilduvaid tehnoloogiaid, millega kahaneb paljangu võimalus.

4.2.3 DMZ-võrgus tuuakse mitteusaldatud host tulemüürist "sissepoole", kuid paigutatakse omaenda võrku (tulemüürihost ühendab seejärel kolm võrku). See suurendab mitteusaldatud hosti turvalisust, töökindlust ja käideldavust, kuid ei suurenda usaldustaset selleni, mida teised "sisemised" hostid võivad lubada. Teised mitteusaldatavad hostid teiste eesmärkidega, nt avalik veebisait või FTP-server, saab hõlpsasti paigutada DMZ-võrku, tekitades avalike teenuste võrgu.

4.2.4 Mõnikord kasutatakse DMZ teostamiseks ühte tulemüüri kolme võrguadapteriga. Esimene adapteritest on ühendatud välisvõrku, teine sisevõrku ja kolmas DMZ-võrku. Selline seadistus ei kaitse toimivalt teenuse degradeerumise eest ummistusründe käigus.

Internet	Tulemüür	DMZ (topeltliidesega) eth0/eth1 (SMTP/WWW/DNS, jne)	Sisevõrk	Usaldatud seadmed
liiklus →	liiklus →←	liiklus →←	liiklus →←	liiklus ←

4.2.5 DMZ-de eelised ja kaalutlused:

• DMZ teostamiseks vajalike lisaarvutite riist- ja tarkvara hind

• Jõudluse väike langus

• DMZ teostamise ajakulu

• DMZ lisamise tõttu süsteemi tabava katkestuse hind

• Vähenenud kättesaadavus ründajale.

4.3 DMZ kahe tulemüüriga konfiguratsioonis

4.3.1 Organisatsiooni sisevõrku saab täiendavalt isoleerida ebausaldatavatest võrkudest, lisades teise tulemüürihosti. Kui ühendada ebausaldatav võrk ühe tulemüürihostiga, organisatsiooni sisevõrk teisega ning tekitada DMZ nende vahele, siis peab liiklus sisevõrgu ja Interneti vahel läbima kaks tulemüüri ja DMZ.

4.3.2 Laiema definitsiooni järgi mõeldagu Interneti protokollil (IP) põhinevale infrastruktuurile välisvõrgu (väline pool) ja sisevõrgu (sisemine pool) vahel. Selline infrastruktuur sisaldab harilikult mitmesugust tüüpi seadmeid: võrguseadmed (nt marsruuterid), süsteemid (nt rakendused nagu e-mail või veebiteenuseid käitavad serverid) ja muidugi turvaseadmed (nt tulemüürid). Tulemüüri iga liidest peetakse vastavaks erinevale segmendile infrastruktuuris, mida nimetatakse DMZ-võrguks.

4.3.3 Igas sellises arhitektuuris kasutatakse tulemüüre, et kontrollida pääsu võrgu piiril, peamiselt eesmärgiga kaitsta võrku ebausaldatava võrgu eest. Tulemüüre, mis on paigaldatud täielikult sissepoole võrku, saab kasutada ka vastastikuseks kaitse tagamiseks selle võrgu alamvõrkudes. Pääsu kontrollimine sisemiste alamvõrkude vahel ei erine pääsu kontrollimisest võrgu ja Interneti vahel, seega saab kõiki eelpoolnimetatud arhitektuure kasutada ka sisemise tulemüüri arhitektuuridena.

4.3.4 Mitmekihilises arhitektuuris on tulemüüri funktsioonid jagatud väikese arvu hostide vahel, mis on tavaliselt ühendatud jadamisi, nii et nende vahele jäävad DMZ-võrgud. Sellist meetodit on raskem kavandada ja käitada, aga ta saab pakkuda oluliselt kõrgemat turvalisust, kuna teostatavad kaitsevahendid on mitmekesisemad. Kuigi see on kallim, oleks mõistlik kasutada erinevaid tehnoloogiaid igas tulemüürihostis, sest see vähendab riski, et sama teostus- või seadistusviga esineb igas kihis. Selline meetod vähendab võimalust, et tekib liiasus või suurem turvarike. Seda tüüpi arhitektuuri kõige levinum kavandamisviis on Interneti tulemüür, mis koosneb kahest hostist, mis on ühendatud läbi ühe DMZ-võrgu.

4.4 Proksi

4.4.1 Proksisid kasutatakse keskkondades, mis nõuavad tugevamaid autentimismeetodeid ja häid logimisvõimalusi, kuna iga proksiagent suudab nõuda autentimist igalt võrgukasutajalt eraldi. Teisest küljest nõuavad need täiustatud turvavõimalused rohkem töötlusvõimsust, mis muudab nad sobimatuks keskkondadesse, kus on nõutud suur ribalaius. Tulemüüris peab olema spetsiaalne agent iga rakenduse liikluse jaoks. Agendid kasutavad e-mailide ja veebi sisu analüüsimiseks järgmisi meetodeid.

• Java-aplettide, ActiveX-rakenduste ja JavaScripti filtreerimine

• Osade MIME-tüüpide blokkimine

• Viiruste ja makroviiruste skännimine

• Rakenduse käskude blokkimine

• Kasutaja määratud blokkimisfunktsioonide kasutamine

5. RISKID, MIDA TULEMÜÜRID OHJELDAVAD

5.1 Tarkvara nõrkustel põhinevad ründed

5.1.1 Sellise ründe eesmärk on muuta server sama hästi kui väljalülitatuks (teenusetõkestusrünne, *DoS*), kuid võib esineda ka volitamata pöördus.

5.1.2 Üks kõige mõjusamaid ründetüüpe on puhvri ületäitmine. Ta pole seotud konkreetse rakendusega ja ta kasutab avalikult teadaolevaid tarkvara programmivigu (puuke) või nõrkusi, et tekitada veaolukord programmis, mida kasutatakse mõne teenuse käsitsemiseks. Probleem saab tavaliselt alguse sellest, kui ületäitumise tingimus kirjutab üle osa mälust, mida programm kasutab. Viirus *Code Red* on näidis ründest, mis kasutab ära sellist nõrkust.

5.1.3 Kataloogirünne on suunatud veebiserverite vastu eesmärgiga saada juurdepääs failisüsteemidele väljaspool volitatud lehekülgi. Selle tulemus võib olla volitamata juurdepääs andmetele või volitamata koodi käivitamine. Mõnes tarkvara vanemas versioonis piisas, kui kasutati URL-i kujul http://server/../../. Viirus *NIMDA* on näidis ründest, mis kasutab ära sellist nõrkust.

5.1.4 Lähtekoodi paljastamise rünne on suunatud veebiserverite vastu, mis töötlevad dünaamilisi lehekülgi. Ründega üritatakse saada juurdepääs lähtekoodile, mis võib sisaldada paigaldusteavet, näiteks kasutajate identifikaatoreid ja andmebaaside paroole. Sellist laadi rünnet saab sooritada, pöördudes spetsiaalselt konstrueeritud URL-i poole, mida server töötleb vigaselt või mis laseb serveril käivitada mõne tarkvarakomponendi, mis võib sisaldada programmivigu.

5.1.5 MIME-nõrkuste rünnak on suunatud meiliklientide ja -teenuste ning mõnel juhul ka brauserite vastu. Ründe käigus modifitseeritakse päiseid, et esile kutsuda teatud olukordi, näiteks teenusetõkestus või rakenduste käivitamine. Mõned kohaldatavad meetmed on järgmised.

• Pidev avaldatud programmivigade ja nõrkuste uus läbivaatus ning turvapaikade ja tarkvarauuenduste paigaldamine;

• Protseduurid, millega kontrollida süsteemi ja rakenduste logisid, et ründeid avastada.

5.2 Töötlusvõimsusel põhinevad ründed

5.2.1 SYN-tulvad on mõeldud tõrgete tekitamiseks programmis, mis käsitseb teenust. Kõige lihtsamal kujul kirjutavad nad üle mälu, mida kasutavad andmed või programmikood, tekitades niiviisi tõrke. Ohtlikumal kujul käivitatakse rünnete käigus ründaja antud programmikood. Kuna tavaliselt käitatakse teenuseid kõrgel privileegitasemel, kujutavad seda tüüpi ründed suurt ohtu. Tavaliselt sisaldavad paketid võltsitud lähteaadressi. SYN-tulvad tekitavad kaks põhilist probleemi: ribalaiuse puudus ja TCP-ühenduste tabeli kasv serveris. Meetmed, mida saab rakendada seda tüüpi rünnete vastu (kuigi neil ei saa olla täielikku toimet) on järgmised.

• Seadistada tulemüürid, et avastada ja välja filtreerida võltsitud aadressid

• Häälestada ühenduse parameetrid, näiteks taimaudid ja ootel ühenduste arv, et vältida TCP-ühenduste tabeli liigset kasvu.

5.2.2 UDP-tulvamine on eelnevale sarnane. Peamine erinevus on, et UDP ei kasuta ühenduste mõistet. Rünne põhineb hõivatud ribalaiusel ning lõpptulemusena ka ressurssidel, mida server kasutab pakettidele vastamiseks.

5.2.3 ICMP-tulvad on minevikus olnud ühed kõige efektiivsemad ründed. Rünnete täiustamiseks kasutavad nad ära konfiguratsiooniprobleeme. *Smurf*, üks tuntumaid rakendusi, põhineb teiste võrkude kasutamisel, et rünnata lõppsihtmärki.

5.2.4 Hajusad ummistusründed (*DDoS*) on mõeldud sihtmärgiks valitud saidi tulvamiseks ühe või rohkema teenusetõkestusründega (*DoS*). Tarkvara- või konfiguratsioonivigu ära ei kasutata. Rünne põhineb ribalaiuse suuremahulisel kasutamisel ning nõuab, et ründes osaleksid (sajad) varasemalt mõjutatud võrgu sõlmpunktid. Sellise ründe vältimiseks pole kuigi palju võimalusi. Mõned meetmed, mida saab rakendada, on järgmised.

Protseduur P6. Tulemüürid (jätkub)

• Filtreerida pakette;

• Anda mõistlik kinnitus, et omavahel ühendatud saitide nõrkused on niivõrd ohjeldatud kui võimalik;

• Reguleerida parameetreid, et ohjeldada TCP-ühenduste tabeli liigset kasvu.

6. TULEMÜÜRIDE LÄBIVAATUSE PROTSEDUURID

	Soovitatavad protseduurid	√
Eelinfo kogumine — Need on näited teabest, mida saab koguda audititöö kavandamiseks.	Hankida turvapoliitikad.	
	Hankida tulemüüri turvapoliitika.	
	Välja selgitada teenused, mida tulemüür peaks kaitsma, ning sooritada nende tundlikkuse üldine kaalutlemine, võttes arvesse CobiT-i seitse infokriteeriumi.	
	Välja selgitada kehtestatud riski kaalutlemise protsess, et tuvastada peamised ohuallikad ja ohtude esinemise tõenäosus.	
	Luua arusaam sellest, kuidas kasutatakse tehnoloogiat, sealhulgas kehtestatud turvameetmeid nagu autentimismeetodid, turvahaldus ja riistvara hooldus.	
	Välja selgitada protseduurid, mida kasutatakse süsteemiarenduse elutsüklis rakenduste kogumi jaoks, mida kasutatakse välisest võrgust (need, mille poole pöördutakse otse ja need, mida nad kasutavad läbi liideste) ja tulemüüri süsteemitarkvara jaoks.	
	Kindlaks teha kehtestatud logimisfunktsionaalsus.	
	Välja selgitada protseduurid, mida kasutatakse reeglite baasi korrashoiuks.	
	Välja selgitada protseduurid, mida kasutatakse uute programmivigade või kasutatava tarkvara nõrkuste seireks.	
	Välja selgitada protseduurid, mida kasutatakse süsteemi- ja rakenduse logide läbivaatuseks, et avastada ründeid.	
	Välja selgitada protseduurid, mida kasutatakse tehnilise ja turvaintsidentidega seotud teabe jagamiseks naabersaitidega.	
	Välja selgitada konfiguratsioonihalduse protseduurid.	
Riski kaalutlemine	Täpsustada läbivaatuse ulatus, kasutades teavet, mis on olemas teenuste, mida tulemüür on mõeldud kaitsma, tundlikkuse kohta ning tuvastatud riskide ja nende esinemise tõenäosuse kohta.	
Täpne plaanimine — Kõik juhtimise eesmärgid, mida saab tuvastada CobiTi protsesside valimise tulemusel, saab läbi vaadata tavalise paigaldusaegse läbivaatusega. See osa sisaldab teatud eriprotseduure, mida võib kaasata tulemüüri paigalduse läbivaatusesse. Need on näited valdkondadest, mida kaasata läbivaatusesse.	IDS-i paigalduse jaoks tuleb läbi vaadata: analüüs, mis tehti olemasoleva võrgu hindamiseks, sisenemispunktide tuvastamine, tulemüüride lubatava liikluse liigid, sisseviidud analüüsireeglid, kehtestatud alarmide ja teavituste skeem.	
	Läbi vaadata iga DMZ eraldiseisvana, arvestades teisi kas erineva võrgu või arvutina. Sellist metoodikat kasutades tuleks hinnata konfiguratsiooni ja reegleid kõikide DMZga seotud võrkude liikluse suhtes.	
	Läbi vaadata protseduurid, mida kasutatakse, et seirata turvalisusega seotud infoallikaid (peamiselt veebisaidid ja spetsiifilised allikad) ning tuvastada uusi ründeliike, näiteks programmivigu. Tuleks mõelda kinnituse saamisele selle kohta, kas kõik kättesaadavad turvapaigad on kehtestatud.	
	Läbi vaadata süsteemiarenduse elutsükli kehtestatud meetmed (näiteks kohustuste eraldamine, algatamine ja testimine) selle suhtes, mis programmikoodi käivitatakse tulemüüritarkvara osana ning rakenduste suhtes, mis on tehtud avalikuks võrgu välispoolele.	
	Läbi vaadata autentimismeetmed, millega kontrollitakse juurdepääsu välisvõrgust.	

Protseduur P6. Tulemüürid (jätkub)

	Läbi vaadata seadmete haldamiseks kasutatavad protseduurid (sealhulgas vähemalt füüsiline ligipääs ja süsteemiülemate paroolid, et näiteks vähendada riski ühenduste manipuleerimiseks volitamata ligipääsu kaudu).	
	Läbi vaadata protseduurid, millega reguleeritakse (süsteemiülemate või tarnijate) kaugpöördust võrguseadmete haldamiseks.	
	Läbi vaadata protseduurid, et logid vaadataks üle toimivalt ja õigeaegselt ning käsitletaks potentsiaalselt kahjulikku liiklust.	
	Läbi vaadata protseduurid võimalike või toimivate rünnete käsitlemiseks.	
	Läbi vaadata reeglipõhise hoolduse protseduurid, näiteks vaadata läbi juurdepääs hooldusfunktsioonidele, nõuete protseduuridele, uute või muudetud reeglite testimisele, üleviimisele tootesse ning dokumenteerimisele. Teha kindlaks, kas on kehtestatud formaalne ja kontrollitud protsess, millega sooritada nõudmine, läbivaatus ja heakskiit, ning tulemüüri lisamine ja muudatused tootmiskeskkonda üle viia. Täpsemalt: 1. Teha kindlaks, kas formaalne nõue sisaldab tegevusalast eesmärki ja rahastajat, esitamise kuupäeva ja reegli vajaduse kestust. 2. Teha kindlaks, kas läbivaatuse sooritab tehniliselt pädev isik, kes mõistab reegliga seotud riski. Läbivaataja peaks dokumenteerima riski kogu teabe-infrastruktuuri kaitsmise suhtes. 3. Teha kindlaks, kas heakskiidu annavad nii tulemüüri ülema juht või ülevaataja kui ka asjakohane tegevusala juht. Taotlus tulemüürireegli kohta peab saama ametliku kinnituse. 4. Enne tulemüürireegli viimist tootmiskeskkonda tuleb teha kindlaks, kas ta on eelnevalt testkeskkonnas formaalselt testitud. Kus võimalik, tuleks testida teenuste seisakuid (näiteks tehes kindlaks seadme ebatavalised seisuajad kohtades, kus oli nõutud muudatust).	
	Läbi vaadata riskihalduse protseduurid.	
	Välja selgitada kesksed rikkepunktid.	
	Läbi vaadata olemasolev virtuaalne privaatvõrk (vaata ISACA suuniseid virtuaalsete privaatvõrkude kohta).	
	Läbi vaadata läbistustestide sooritamise plaan ning testide uuesti sooritamise kriteeriumid juhuks, kui tehakse muudatusi. Katta testimisel avastatud riskid.	
	Välja selgitada kõik kehtestatud filtreerimisreeglid (et teha kindlaks, kas nad pööravad tähelepanu kõigile turvapoliitika aspektidele ja teistele asjakohastele ohtudele, mis tuvastati riskianalüüsi käigus). Kontrollida, et üleüldine tulemüürireegel piirab juurdepääsu, välja arvatud siis, kui reeglid seda spetsiaalselt lubavad.	
	Läbi vaadata protseduurid, mis käsitlevad parandatud reeglite testimist enne nende üleviimist tootmiskeskkonda.	
	Läbi vaadata meetmed, mis käsitlevad füüsilist juurdepääsu tulemüürile ja võrguseadmetele, mis ühendavad teda võrkudega.	
	Läbi vaadata protseduurid, mida kasutatakse uue tarkvara testimisel ja tema turvasätete konfigureerimisel nii, et saavutada määratud turvapoliitikate täitmine.	
	Läbi vaadata avariitaaste- ja toibumisprotseduur. Tuleks arvesse võtta tõrkesiirdeseadme olemasolu, mis toetab tulemüüri talitlusfunktsioone (kuna tulemüüri teenustel on tavaliselt kõrged käideldavusnõuded).	
	Läbi vaadata konfiguratsioonihalduse protsessid.	

Protseduur P6. Tulemüürid (jätkub)

Oleku jälgimine/dünaamiline pakettide filtreerimine (SI/DPF)	Dokumenteerida, kuidas SI/DPF mõjutab teise tulemüüri tagatavaid meetmeid olukorras, kus SI/DPF kasutatakse piiri-tulemüürina ja tema taga on veel üks tulemüür.	
	Saada kinnitus, et programmi muutmise meetmed (eriti testimismeetmed) rakendatakse kõikidele API-dele, juhul kui kasutatakse SI/DPF-i API-sid (et käivitada organisatsioonis tulemüüri operatsioonisüsteemile kirjutatud koodi).	
	SI/DPF kasutab olekutabeleid ja programmeeritud instruktsioone. Ta kasutab teavet paketipäisest ja -sisust kuni rakenduskihini välja. Teave töödeldakse ja talletatakse, et anda tulemüürile kontekst liikluse klassifitseerimiseks. Peamine eesmärk on tuvastada paketid, mis kuuluvad avatud ühendusse ning avada või sulgeda spetsiifilisi porte vastava liikluse jaoks. Tuleb kavandada ja sooritada sellise liikluse testimine, mida SI/DPF mõjutab, et saada kinnitus tema õige talitluse kohta.	
	Näited aspektidest, mida filtrite läbivaatusel arvesse võtta: lüüsid, FTP-seansid, X-Windows, DNS, fiksaadressid. Tuleb saada kinnitus järgneva kohta. • Juurdepääs on lubatud ainult aadressidele, mis on mõeldud väljaspoolt pöördumiseks. • Volitamata teenuseid nagu FTP ja Telnet on keelatud kasutada. • Juurdepääs teatud portidele on keelatud. • Lubatud on ainult paketid, mis tulevad volitatud saitidelt välisvõrgus. • Kogu lähtemarsruuditud liiklus heidetakse kõrvale.	
	Hinnata pääsukontrolli reegleid või teisi meetmeid, mis on kehtestatud, et heita kõrvale soovimatut sidet loovad paketid (näiteks ummistusründed seadmete vastu).	
	Saada kinnitus, et on kehtestatud reeglid, millega välditakse IP spuufimist.	
	Saada kinnitus, et kasutatakse NATi, et edastatakse ainult paketid, mis pärinevad kindlatelt lubatud IP-aadressidelt sisevõrgus, ja et sisenev liiklus on lubatud ainult siis, kui on loodud kehtiv ühendus.	
Pakettide filtreerimine	Kui marsruuterit kasutatakse piiri-tulemüürina ja tema taga on veel üks tulemüür, tuleb dokumenteerida, kuidas see mõjutab teise tulemüüri tagatavaid meetmeid.	
	Saada ettekujutus sellest, kuidas rakendatakse pakettide filtreerimist, pidades silmas, kuidas kasutatakse paketipäisest pärinevat teavet lähte- ja sihtpunkti, protokolli ja pordi kohta.	
	Kaalutleda toimet meetmetele ning välja selgitada kesksed riskialad, mis tekivad pakettide filtreerimise tulemusel. Tuleb saada kinnitus järgneva kohta. • Juurdepääs on lubatud ainult aadressidele, mis on mõeldud väljaspoolt pöördumiseks. • Volitamata teenuseid nagu FTP ja Telnet on keelatud kasutada. • Juurdepääs teatud portidele on keelatud. • Lubatud on ainult paketid, mis tulevad volitatud saitidelt välisvõrgus. • Kogu lähtemarsruuditud liiklus heidetakse kõrvale.	
	Kavandada ja sooritada sellise liikluse testimine, mida mõjutab pakettide filtreerimine.	
	Hinnata reegleid, mis on kehtestatud, et heita kõrvale soovimatut sidet loovad paketid (näiteks ummistusründed seadmete vastu).	
	Saada kinnitus, et on kehtestatud reeglid, millega välditakse IP spuufimist.	
	Saada kinnitus, et kui kasutatakse NATi, ei saa teha otsemarsruutimist sisemistele IP-aadressidele.	

Protseduur P6. Tulemüürid (jätkub)

Pakettide filtreerimise loomupärased riskid	Logimissuutlikkus on puudulik või puuduv, mistõttu süsteemiülemal võib olla raske tuvastada, kas marsuuter on rikutud või ründe all.	
	Tihti on pakettide filtreerimisreegleid raske põhjalikult testida, mis võib saidi jätta avatuks testimata nõrkustele.	
	Kui nõutakse keerulisi filtreerimisreegleid, võivad need muutuda hallatamatuks.	
	Iga host, mis on Internetist otse kättesaadav, vajab oma koopiat täiustatud autentimismeetmetest.	
Hübriidtulemüürid	Dokumenteerida, kuidas hübriidtulemüüride kasutamine mõjutab võrguliiklusele rakendatavaid turvameetmeid.	
	Saada ettekujutus sellest, kuidas kasutatakse kolme tulemüürimetoodikat (pakettide filtreerimine, oleku filtreerimine ja proksid). Tuleb kindlaks teha loogika, mille alusel edastatakse liiklust tulemüüri igasse protsessi.	
	Kaalutleda toimet meetmetele ning välja selgitada kesksed riskialad, mis tekivad hübriidmeetodi kasutamisel. Kaalutleda otsustusloogikat, mille põhjal selgitatakse välja, millist tulemüürimeetodit kasutada millist tüüpi liikluse jaoks.	
	Kavandada ja sooritada sellise liikluse testimine, mida mõjutab SI/DPF, võttes arvesse järgmised reeglid. • Saada kinnitus, et on olemas kooskõla sarnaste protokollide suunamisel samasse protsessi hübriidi piires. • Saada kinnitus, et kõik oleku filtreerimisel kasutatavad API-d on ohjatud. • Saada kinnitus, et proksi protsess säilitab lahusust liikluse ja rakenduse vahel. • Saada kinnitus, et läbilaskevõime ja ajakulu turvameetmete rakendamiseks on sobivalt tasakaalus.	
	Hinnata pääsukontrolli reegleid või teisi meetmeid, mis on kehtestatud, et heita kõrvale soovimatut sidet loovad paketid (näiteks ummistusründed seadmete vastu).	
Proksi-tulemüürid	Proksi-tulemüür võib olla eraldiseisev seade, või teenus, mida käitatakse mitmeotstarbelisel tulemüüriseadmel. Tema eesmärk on lisada erilisi töötlusmeetmeid ühe konkreetse liiklusetüübi jaoks.	
	Saada ettekujutus sellest, kuidas kasutatakse proksit -- millist liiklust saadetakse läbi proksi ja millised seadmed võtavad vastu väljundi.	
	Saada kinnitus, et kogu sedalaadi liiklus, mida proksi töötleb, peab voogama läbi proksi-tulemüüri. Kõikide seadmete kohta seespool proksit tuleb saada kinnitus, et nad aktsepteerivad proksitavat tüüpi liiklust ainult proksiseadme aadressilt.	
	Kavandada ja sooritada sellise liikluse testimine, mida mõjutab proksi, võttes arvesse järgmist. • Tuleb saada kinnitus, et kogu liiklus on suunatud proksile • Tuleb saada kinnitus, et kogu proksitavat tüüpi liiklust töödeldakse ainult proksi aadressilt.	
	Hinnata proksi logide läbivaatuse protseduure ja nende protseduuride toimivust, millega käsitletakse logide põhjal tuvastatud võimalikke probleeme.	

Protseduur P6. Tulemüürid (jätkub)

DMZ — Tuleks mõelda kolme segmendiga DMZ-võrgule: üks kehastab ühendust väljapoole, teine kehastab ühendust sissepoole ja kolmas, DMZ-segment, koosneb IP-alamvõrgust, kus asuvad süsteemid, millele on väljast juurdepääs.	Kontrollida, et tulemüür on väljaspoole nähtamatu.	
	Kontrollida, et DMZ-segmendis asuvad süsteemid on väljaspoole nähtamatud.	
	Kui välised teenuseandjad saavad sooritada rikkeotsingut seadmetel, mis asuvad DMZ-võrgu piiril, kus luuakse ühendus teenusepakkujatega (ja välispoolega üldiselt), tuleb saada kinnitus järgnevas. • Testidega on tuvastatud täpne ulatus, milleni võib kaardistada seda, mis asub DMZ-võrgus • On loodud arusaam võimalikust vallutusefektist.	
	Läbi vaadata DMZ-võrk, et anda mõistlik kinnitus selle kohta, et välised olemid ei saa hallata ega konfigureerida järgmist. • Tulemüür • Võrguseadmed ja süsteemid DMZ-võrgus. (Kui mis tahes põhjusel (näiteks rikkeotsinguks) saab pöörduda väljaspoole paistva segmendi võrguseadmete poole, näiteks marsruuterite poole, mis ühenduvad teenuseandjatega, tuleb kontrollida, et on olemas meetmed selle kohta, kes saab hallata/konfigureerida neid seadmeid.)	
	Kontrollida, et väljaspoolt paistva segmendi võrguseadmetes on kehtestatud pääsukontrolli reeglid, mille eesmärk on keelata soovimatut sidet loovad paketid (näiteks ummistusründed).	
	Läbi vaadata tulemüüri reeglid ja selle käigus kontrollida, et iga pakett on vaikimisi keelatud, välja arvatud siis, kui on olemas spetsiifiline reegel, mis lubab paketil edasi liikuda – kuid ainult sihtsüsteemini DMZ-segmendis.	
	Saada kinnitus, et süsteemid DMZ-segmendis on seadistatud nii, et nad ei saa sidet pidada ühegi teise süsteemiga väljaspool DMZ-segmenti muidu kui tulemüüri vahendusel. Kui on tehtud erandeid, tuleb hinnata spetsiifilisi riske, õigustust eranditele ja tasakaalustavaid meetmeid.	
	Saada kinnitus, et süsteemid DMZ-segmendis on seadistatud nii, et nad ei saa algatada sidet sisevõrguga. Jällegi, kui on tehtud erandeid, tuleb hinnata spetsiifilisi riske, õigustust eranditele ja tasakaalustavaid meetmeid.	
	Saada kinnitus, et võrguseadmed, tulemüürid ja süsteemid DMZ-võrgus on seadistatud nii, et marsruutimine ükskõik millise seadmete, tulemüüride ja süsteemide võimaliku kombinatsiooni vahel on selgelt defineeritud: • Kõik marsruudid, mis sisenevad DMZ-võrku, läbivad seda ja väljuvad sealt, on kergesti tuvastatavad. • Kehtestatud marsruutimine on vähim, mis on vajalik volitatud sidevoogude toeks. (Kui kasutatakse mittemarsruuditavaid sideprotokolle, tuleb saada kinnitus, et nende eesmärk ühtib DMZ-võrgule esitatud turvapoliitika nõuetega.)	
	Kui kasutatakse NAT-i, tuleb anda mõistlik kinnitus, et ta töötab viisil, mis on kooskõlas turvapoliitika nõuetega ja et vastutavad isikud taassertifitseerivad konfiguratsiooni perioodiliselt.	
	Saada kinnitus, et tulemüür on seadistatud järgmiselt. • Keelatakse kõik paketid, mis sisenevad väljastpoolt, aga mille IP-lähteaadressid pärinevad näiliselt sisevõrkudest. • Keelatakse kõik paketid, mis tulevad seestpoolt, aga mille IP-lähteaadressid ei pärine seestpoolt.	
	Saada kinnitus, et tulemüürireeglid avastavad välised katsed sondeerida tavaliselt sondeeritavaid porte (olenemata sellest, kas süsteemid üldse kuulavad sellistel portidel).	
	Saada kinnitus, et tulemüür on seadistatud nii, et ta ei saada ühtegi sõnumit vastuseks sisenevale keelatud paketile.	

Protseduur P6. Tulemüürid (jätkub)

	Saada kinnitus, et tulemüüri on testitud, sondeerides iga segmenti (sealhulgas DMZ-segmenti) igast muust segmendist, et tuvastada, millised paketid pääsevad läbi või ei pääse. Tuleb anda mõistlik kinnitus, et tulemused on kooskõlas üldise turvapoliitikaga.	
	Saada kinnitus, et kõik reeglid tulemüüris on kooskõlas turvapoliitikaga. Teisisõnu tuleb anda mõistlik kinnitus selle kohta, et kooskõlalisus poliitikaga on tõendatav, analüüsides potentsiaalselt lubatavate pakettide järgmisi komponente: protokoll, lähtesüsteemi IP-aadress, sihtsüsteemi IP-aadress, lähteport ja sihtport. Näiteks peaks sihtsüsteemi ja -pordi kombinatsioon reeglis muutuma arusaadavaks, kui mõelda sihtsüsteemi funktsioonile DMZ-segmendis. Reegel peaks kaitsma ka tulemüüri ennast; ta peaks olema kooskõlas funktsioonidega, mida annavad süsteemid DMZ-segmendis ning ta peaks lubama süsteemidel sisevõrgus algatada sidet süsteemidega DMZ-segmendis, või lubama süsteemidel DMZ-segmendis vastata sidele, mis on algatatud seestpoolt. Kui reeglibaasis on reegleid liiga palju, et neid testi käigus läbi vaadata, võib see osutada halvastiprojekteeritud turvaarhitektuurile, mis muudab haldamise ja nõuetekohase katvuse tagamise väga raskeks.	
	Saada kinnitus, et tulemüüri reeglid keelavad kõik paketid, mis sisaldavad TCP- või UDP-porte kõrgema numbriga kui 1023, et anda mõistlik kinnitus, et rakenduse porte kasutatakse ettenähtud viisil. Kui mitte, tuleb hinnata spetsiifilisi riske, õigustust ja tasakaalustavaid meetmeid.	
	Kui DMZ-võrk sisaldab mitut füüsilist tulemüüri kõrgkäideldavuse, liiasuse või tõrkesiirde eesmärgil, tuleb saada kinnitus, et käitatavad tulemüüride konfiguratsioonid on võrdväärsed.	
Täiendavad kesksed punktid arvessevõtmiseks		
Konfiguratsioon	Tulemüüri ei tuleks paigaldada või ta ei peaks käitama teenuseid DNS, e-mail, serveri koormuse tasakaalustamise teenus ega ükskõik millised muud teenused või tarkvara, mis ei seondu tulemüürispetsiifiliste funktsioonidega.	
	Tulemüürid tuleks konfigureerida nii, et nad varjaks sisemise salastatud DNS-teabe väliste võrkude eest.	
	Välised tulemüürid peaks filtreerima sisenevaid SNMP-päringuid.	
	Marsruuteri pääsuloendid ei taga kaitsetaset, mida nõutakse tulemüürilahenduselt. Marsruuterit tuleks kasutada osana tulemüürilahendusest (näiteks esmase Interneti-poolse filtrina). See tagab ühenduvuse ja vähendab osaliselt tulemüüri koormust, edastades üksnes vajalikke porte, selle asemel, et lasta tulemüüril filtreerida iga üksikut porti. (Siiski peaks igaks juhuks olema kehtestatud reeglid, mis blokeerivad kasutamata pordid tulemüüris.)	
	Tulemüürid tuleb konfigureerida „tõrkel sulguvaks“.	
	Teavet sisevõrgu kohta tuleb varjata väliste allikate eest.	
	Tulemüürid tuleb konfigureerida „keelama kõiki teenuseid, välja arvatud neid, mis on eksplitsiitselt lubatud“.	
	Tuleb transleerida selliste sisevõrgu sõlmpunktide aadressid, millel on lubatud sidet pidada väliste võrkudega.	
	Kui võimalik, tuleb vältida UDP-põhiseid teenuseid.	
	Tuleb skaneerida, filtreerida või blokeerida Java, JavaScript ja ActiveX.	
	Protokoll NNTP tuleb piirata kasutajatega, kes teda vajavad. Sellel peaks olema formaalne õigustus.	
	Võimalusel tuleb marsruutimisprotokollide asemel kasutada staatilist marsruutimist.	
	Hostile, kus asub tulemüür, tuleb rakendada tugevad turvapoliitikad.	
	Piirata juurdepääsu tulemüüri genereeritud logidele, et vältida nende volitamatut kustutamist või muutmist.	

Protseduur P6. Tulemüürid (jätkub)

	Tulemüürisüsteemi komponentidele tuleb rakendada kõik turvaparandused ja muu seesugune.	
	Kindlaks teha, kas on kehtestatud protseduurid, millega kontrollida turvapoliitikaid (näiteks läbistustestimine, reeglibaasi käsiläbivaatus, operatsioonisüsteemi turvaläbivaatused jms).	
	Kontrollida, kas on olemas vahendid tulemüürisüsteemi tundlike failide tervikluse seireks.	
Seire, revisjon ja intsidendikäsitlus	Pidevalt seirata tulemüüri hoiatusi.	
	Logida kõik tulemüüri tegevused.	
	Kindlaks teha, kas tundlike või kõrge riskiga ühenduste jaoks on täiendavad kaitsevahendid, näiteks sissetungi tuvastamise süsteemid.	
Varundamine ja taaste	Kontrollida, kas tulemüüride pidevuse plaanid on kooskõlas teiste kõrgkäideldavusega teenuste pidevusplaanidega, kuna tulemüürid on tavaliselt komponendid, mis seonduvad kõrgkäideldavusnõuetega teenustega.	

7. JÕUSTUMISKUUPÄEV

7.1 See protseduur kehtib kõikidele IS audititele, mis algavad või toimuvad pärast 1. augustit 2003. Täielik sõnaseletuste kogu asub ISACA veebilehel *www.isaca.org/glossary*.

LISAD

Toetumine COBITile

Järgnev valik kõige asjakohasematest materjalidest COBITis, mida saab rakendada konkreetse auditi ulatuses, põhineb spetsiifiliste COBITi IT-protsesside valikul ja COBITi teabekriteeriumite arvessevõtmisel.

See protseduur toetub järgmistele peamistele COBITi protsessidele:

- PO9 – Kaalutleda riskid
- TT4 – Tagada pidev teenus
- TT5 – Tagada süsteemide turvalisus (5.20 on spetsiifiline tulemüüride juhtimiseesmärk)
- HE6 – Hallata muutusi

See protseduur toetub järgmistele COBITi protsessidele:

- HE2 – Hankide ja hooldada rakendustarkvara
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda (juhtimiseesmärgid 3.4, 3.5, 3.6 ja 3.7)
- HE4 – Koostada ja hooldada IT-protseduurid (COBIT v3)
- HE5 – Paigaldada ja akrediteerida süsteemid (COBIT v3)

Protseduur P6. Tulemüürid (jätkub)

- TT1 – Määratleda ja hallata teenusetasemeid
- TT2 – Hallata kolmanda osapoole teenuseid
- TT3 – Hallata sooritust ja suutvust
- TT10 – Hallata probleeme
- PO2 – Määratleda infoarhitektuur
- S3 – Saada sõltumatu kinnitus (COBIT v3)

Kõige asjassepuutuvamad kriteeriumid on:

- esmajärjekorras: terviklus, käideldavus ja konfidentsiaalsus;
- teises järjekorras: toimivus ja usaldatavus.

Allikad

Järgnevas loetelus on mõned kasulikud allikaviidetena ja üksnes näite-eesmärgil kasutatud leheküljed.

CERT/CC (Computer Emergency Response Team/Coordination Center), *www.cert.org/tech_tips/packet_filtering.html*

Checkpoint FW1, *www.checkpoint.com/products/security/index.html*

Cisco Pix, *www.cisco.com/warp/public/cc/pd/fw/sqfw500/*

Digital Robotics (Internet Firewall 2000), *sysopt.earthweb.com/reviews/firewall/index3.html*

Federal Computer Incident Response Center (FedCIRC) *www.fedcirc.gov*

Firewall Options Chart, *www.networkbuyersguide.com/search/105242.htm*

Guardian, *www.netguard.com/subpages/products.htm*

National Infrastructure and Protection Center, *niap.nist.gov*

NetScreen, *www.netscreen.com/products/*

Network Ice (Black Ice Defender), *www.networkice.com/products/soho_solutions.html*

NIST nõrkuste andmebaas, *icat.nist.gov*

Nokia, *www.nokia.com/securitysolutions/network/index.html*

SANS Institute, *www.sans.org/top20.htm*

Sonic FW, *www.rosser.com.au/products/Sonic/sonproducts.htm*

Symantec/Axent, *enterprisesecurity.symantec.com/content/productlink.cfm#2*

SYN-tulvamise ja IP-spuufimise ründed, *www.cert.org/advisories/CA-1996-21.html*

UDP Port Denial-of-Service Attacks *www.cert.org/advisories/CA-1996-01.html*

Protseduur P6. Tulemüürid (jätkub)

Vabavaralised tulemüüritooted

Sygate, *www.sygate.com/swat/products/default.htm*

Tiny Personal Firewall, *www.tinysoftware.com*

ZoneAlarm, *www.zonealarm.com*

Aruandlustooted tulemüüridele

www.stonylakesolutions.com/sls/insideout.jsp

Levinud riistvaraplatvormid

Dell

HP/Compaq

HP-UX

IBM

Macintosh

Sparc

Sun

Levinud operatsioonisüsteemid

Linux

Macintosh

Netware

UNIX

Windows

Protseduur P7. Korratused ja ebaseaduslikud toimingud

1 TAUST

1.1 Seos ISACA standardite ja suunistega

1.1.1 Standard S3 "Kutse-eetika ja standardid" määrab: "IS audiitor peaks auditiülesannete täitmisel järgima ISACA kutse-eetika koodeksit."

1.1.2 Standard S3 "Kutse-eetika ja standardid" määrab: "Auditiülesannete täitmisel peaks IS audiitor ilmutama vajalikku kutsealast hoolikust, sealhulgas järgima kohaldatavaid kutsealaseid auditeerimise standardeid".

1.1.3 Juhiseid annab suunis G19 "Korratused ja ebaseaduslikud toimingud".

1.1.4 Juhiseid annab protseduur P1 "IS riski kaalutlemine".

1.1.5 Juhiseid annab suunis G15 "Plaanimine".

1.1.6 Juhiseid annab suunis G6 "Kaalukuse kontseptsioonid infosüsteemide auditeerimisel".

1.1.7 Juhiseid annab suunis G2 "Auditi asitõendite nõue".

1.2 Seos COBITiga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

- soorituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?
- IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?
- teadlikkusele: millised on eesmärkide saavutamata jäämise riskid?
- mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusе indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annab käesoleva suunise lisas olev viide COBITile.

1.3 Protseduuride vajadus

1.3.1 IS audiitor ei ole küll otseselt kohustatud avastama ega vältima korratusi, kuid ta peaks kaalutlema korratuste esinemise riski suurust. Riski kaalutlemise ja muude plaanimise ajal sooritatud protseduuride tulemuste abil tuleks määrata ülesande täitmisel sooritatavate protseduuride iseloom, ulatus ja ajastus. IS audiitor peaks kasutama oma kutsealast otsustusvõimet. See dokument on mõeldud aitama IS audiitoril seda eesmärki saavutada.

1.3.2 Audit ei saa garanteerida, et korratused avastatakse. Korratused võivad jääda avastamata ka siis, kui audit on õigesti plaanitud ja läbi viidud.

1.3.3 IS audiitorile võidakse anda teavet oletatava korratuse või ebaseadusliku toimingu kohta ja ta võib kasutada lisateabe kogumiseks andmete analüüsi võimalusi.

2 MÄÄRATLUSED

2.1 Üldkasutatavad terminid

2.1.1 Viga (eksitus) tähendab ettekavatsematut vääresitust või ärajättu.

2.1.2 Korratused on kehtiva halduspoliitika või õigusaktide nõuete sihilikud rikkumised, auditeeritavat ala või kogu organisatsiooni puudutava teabe sihilik vääresitus või ärajätt, suur hooletus või ettekavatsematud ebaseaduslikud toimingud.

2.1.3 Ebaseaduslikud toimingud on õigusnormidega vastuolus olevad toimingud.

2.1.4 Pettus tähendab eksiteele viimist teenimatu või ebaseadusliku rahalise kasu saamiseks.

2.1.5 Nende mõistete vahel ei ole küll selget eraldusjoont, kuid pettuse ja vea vahelise erinevuse määravad kaks elementi: sihilikkus ja kaalukus. Sihilikkust ei saa IS audiitor võib-olla kindlaks teha, seetõttu on määratlevaks teguriks üldiselt kaalukus. Harilikult parandab organisatsioon kaalukad vead, kui need ilmsiks tulevad. Kui aga ilmnenud kaalukat viga ei parandata, muutub ta korratuseks, st ettekavatsematu toiming muutub sihilikuks.

2.1.6 Lihtsuse mõttes on selles dokumendis kasutatud terminit "korratus" kõigis tema tähendustes.

2.2 Kaalukus

2.2.1 Kui IS auditi eesmärk on seotud süsteemide või operatsioonidega, mis töötlevad rahalisi tehinguid, tuleks kaalukuse hindamisel arvestada nende süsteemide kontrolli all olevate varade väärtust või päevas/nädalas/kuus/aastas töödeldavate tehingute väärtust.

2.2.2 Kui rahalisi tehinguid ei töödelda, võib kaalukuse hindamiseks valida mõõdu näiteks alljärgnevate hulgast.

- Süsteemi või operatsiooniga toetatava äriprotsessi elutähtsus.
- Süsteemi või operatsiooni maksumus (riistvara, tarkvara, personal, kolmandate poolte teenused, üldkulud või nende kõigi kombinatsioon).
- Vigade potentsiaalne hind (mida väljendavad näiteks kaotatud müügitulu, garantiitaotlused, tasuvuseta arenduskulud, hoiatuste avaldamise kulud, paranduskulud, tervishoiu- ja ohutuskulud, ülemäära suured tootmiskulud, rohked jäätmed jms).
- Perioodi jooksul töödeldavate pöörduste, tehingute või päringute arv.
- Koostatavate aruannete ja käigushoitavate failide iseloom, ajastus ja ulatus.
- Käideldavate materjalide iseloom ja kogused (näiteks väärtusteta laoarvestuses).
- Teenusetasemeleppe nõuded ja võimalike sanktsioonide rahaline väärtus.
- Sanktsioonid õigusaktide ja lepingute nõuete täitmatajätmise eest.
- Sanktsioonid tervishoiu- ja ohutusnõuete täitmatajätmise eest.
- Korratuste lahendamata jäämise tagajärjed huvipooltele, organisatsioonile või juhtkonnale.

3 VASTUTUS

3.1 Juhtkond

3.1.1 Juhtkond vastutab korratuste vältimist ja avastamist hõlmava sisejuhtimismeetmete süsteemi kavandamise, teostamise ja käigushoiu eest. IS audiitorile peaks olema selge, et juhtimismehhanismid ei välista korratuste võimalust, ning ta peaks piisavalt tundma korratuste teemat, nii et ta saaks välja selgitada tegelikud tegurid, mis võivad soodustada korratuste asetleidmist.

3.1.2 Korratuste avastamise eeltingimused võivad olla järgmised:

- organisatsiooni korratuseriski määramine ta tegutsemis- ja juhtimiskeskkondade uurimise teel;
- põhjalik sümptomite tundmine; nende hulka võivad kuuluda

- volitamata tehingud,

- sularaha liigsus või nappus,

- seletamatud hindade kõikumised,
- dokumentatsiooni puudumine,
- rohked tühistused või tagasimaksed,
- kohustuste lahususe puudumine,
- venitamine: hoiustega viivitamine puudujääkide katmiseks,
- lohelennutus (*kiting*) – pangatšekkide töötluseks kuluva aja ärakasutamine kasu saamiseks[4] mitme pangaga korraga sooritatavate mõlemasuunaliste makseoperatsioonidega,
- kooskõlastamata kontod,
- üksikasjade eiramine,
- väärad kooskõlastused
- väärad kontode kooskõlastused:
  - mingi arvu lisamine kooskõlastuse tasakaalustamiseks,
  - vanade sooritamata maksete üleviimine pikaajalisteks,
- suutmatus tarnida adekvaatseid tooteid või teenuseid,
- manipuleerimine juhtkonna hinnangutega:
  - kulum,
  - kahjude hüvitused,
  - eraldised tulevaseks garantiitööks,
- töötajate vastuseis puhkusele või töökohtade rotatsioonile,
- valvsus nende sümptomite ilmnemise suhtes.

3.2 IS audiitori vastutus

3.2.1 IS audiitor ei ole kutsealaselt vastutav korratuste või ebaseaduslike toimingute vältimise või avastamise eest.

3.2.2 Kui ei ole mingit teavet, mis näitaks IS audiitorile, et on leidnud aset korratus või ebaseaduslik toiming, ei ole IS audiitor seetõttu kohustatud sooritama mingeid protseduure, mis on spetsiaalselt määratud avastama korratusi või ebaseaduslikke toiminguid.

3.2.3 Ülesande lähtetingimustes võidakse aga IS audiitorile esitada erinõue sooritada protseduure, mis on määratud avastama korratusi või ebaseaduslikke toiminguid.

3.2.4 Üks peamisi juhtkonna käsutuses olevaid korratuste ja vigade vältimise ja avastamise meetodeid on toimiv sisejuhtimise süsteem. IS audiitor ei ole üldiselt kohustatud sellele toetuma ja seetõttu seda süsteemi testima, kui seda ei nõua konkreetsed õigusaktid või kokkulepped. IS audiitor peaks aga olema teadlik sellest,

[4] Kõige kahjutumal juhul: lühiajalise ebaseadusliku intressivaba laenu näol. Tõlkija m.

et organisatsiooni sisejuhtimismeetmete nõrkused võivad töötajatel hõlbustada korratuste toimepanemist. IS audiitor peaks olema teadlik ka sellest, et juhtkond võib meetmetest mööduda ja see võib soodustada kõrgemal juhtkonnal pettuste sooritamist. Kui IS audiitorile ilmneb korratus, mis võiks olla pettus, peaks ta taotlema õigusnõustamist edasise tegevuse kohta.

3.2.5 Risk on tõenäosus, et kehtestatud sisejuhtimise süsteem ei väldi või ei avasta sellise toimingu või sündmuse asetleidmist, millel on kahjulik toime organisatsioonile ja ta infosüsteemidele. Risk võib olla ka võimalus, et mingi oht kasutab ära mingi vara või varade rühma nõrkused, põhjustades nende varade kaotuse või kahjustuse. Tavaliselt mõõdetakse riski kahjuliku sündmuse asetleidmise toime ja tõenäosuse mingi kombinatsiooniga. Olemuslik risk on mingi sellise sündmusega seotud risk spetsiaalsete turvameetmete puudumisel. Jääkrisk on sündmusega seotud risk selle sündmuse toimet või tõenäosust vähendavate meetmete rakendatuse korral. Riski kaalutlemine on protsess, millega tuvastatakse ja hinnatakse riskid ja nende võimalik toime.

3.2.6 Rahandusliku auditeerimise ülesande täitmisel peaks IS sisemeetmete hindamisel kaalutlema korratuste riski. Harilikult on selle juhtimiseesmärgi tõukejõududeks järgmised peamised teabekriteeriumid:

- konfidentsiaalsus,
- terviklus,
- täielikkus,
- käideldavus,
- vastavus,
- usaldatavus,
- ebaseaduslikud tehingud,
- ebalegaalsetes maksupelgupaikade kasutamine või neisse investeerimine,
- spekulatiivne investeerimine,
- ebausaldusväärsed süsteemid.

4 AUDITI KAALUTLUSI

4.1 IS audiitorilt võidakse nõuda mõistliku kinnituse andmist sellele, et organisatsioonil on adekvaatsed meetmed korratuste vältimiseks või avastamiseks. Järgnev meelespea on mõeldud ainult näitena ega ole ammendav.

Protseduur P7. Korratused ja ebaseaduslikud toimingud (jätkub)

Korratuste ja ebaseaduslike toimingute uurimine		
PO9 **Hinnata risk** **TT5** **Tagada süsteemide turvalisus** **TT11** **Hallata andmeid**	Kaaluda konsulteerimist kriminalisti või uurijaga.	
	Teha kindlaks äritegevuse iseloom, näiteks varade hoidmine usaldusasutusena ja varasid võidakse kergesti vääralt omastada.	
	Tuvastada asjaolud, mis võivad juhtkonda õigustamatult mõjutada, näiteks aktsiate või eelisostuõiguste kuulumine juhtkonnale ja tulemuspreemiad.	
	Teha kindlaks tulude prognoosi täitmise surve.	
	Teha kindlaks juhtkonna moraalne kindlus.	
	Tuvastada ebatavalised ja/või erisuhetel põhinevad tehingud kolmandate pooltega.	
	Tuvastada tehingud seotud pooltega.	
	Tuvastada ebatavalised tehingud firmadega, kes on registreeritud maksupelgupaikades.	
	Teha kindlaks, kas likviidsus on pingul ja on peaaegu jõutud laenuvõtu piirideni.	
	Tuvastada juhtkonnapoolsed reeglitest möödumised.	
	Tuvastada ebapädev juhtimispersonal.	
	Teha kindlaks, kus puudub kohustuste lahusus.	
	Tuvastada kõrgemale ametnikule antud ülemäärane võim.	
	Tuvastada halvad süsteemid.	
Riski kaalutlemise tulemused	Riski kaalutlemise tulemuste põhjal määrata sellise testimise iseloom, ajastus ja ulatus, mis on vajalik piisavate auditi asitõendite saamiseks eesmärgiga anda mõistlik kinnitus sellele, et on tuvastatud korratused, millel võib olla kaalukas toime auditeeritavale alale või kogu organisatsioonile; on tuvastatud juhtimise nõrkused, mis ei võimalda vältida ega avastada kaalukaid korratusi.	
	Protseduurid, mis aitavad audiitoril avastada ja/või kinnitada korratuste esinemist, keskenduvad tuvastatud suureriskilistele aladele ja võivad põhineda auditikeskkonnas olevatel tingimustel, sealhulgas auditeeritava omadel; selliste hulka kuuluvad organisatsiooni ja juhtkonna hoiakud ja normid turvalisuse ja sisemeetmete suhtes; füüsilise ja loogilise turbe metoodikad; rahalised surved; tegutsemise ja tegevusala keskkonnad, regulatiivne keskkond ja privaatsuskohustused; siseseire meetmed; kasutuselolevad haldusprotseduurid korratuste ja ebaseaduslike toimingute vältimiseks ja avastamiseks; seletamatud toimingud, tasakaaluta olukorrad ja statistilised hälbed; inimressursipoliitikad, mis sisaldavad palkamise ja taustakontrolli protsesse ning ergutuskavasid.	
Analüütilised protseduurid	Väga kasulik korratuste avastamise meetod on oluliste arvväljade jagatiste arvutamine. Väljade valik sõltub vaadeldavast alast, kuid paljude hulgas on ülkasutatavad järgmised jagatised: suurim väärtus vähimaga (uurida ebatavaliselt suuri erinevusi), suurim väärtus suuruselt järgmisega (uurida olulisi kõrvalekaldeid normist), eelmise aasta oma praegusega (aitab keskenduda suurima riski aladele), plaaniline või eelarveline tegelikuga – dispersioonanalüüs, mitme aasta trendi analüüs.	

Protseduur P7. Korratused ja ebaseaduslikud toimingud (jätkub)

Kohustused	Korratuste avastamise puhul peaks IS audiitor hindama nende mõju auditi eesmärkidele ja kogutud asitõendite usaldatavusele.	
	Kui auditi asitõendid näitavad, et võisid aset leida korratused, peaks IS audiitor soovitama juhtkonnal asja detailselt uurida või rakendada asjakohaseid meetmeid.	
	Kui auditi asitõendid näitavad, et korratusega võis kaasneda ebaseaduslik toiming, peaks IS audiitor otsima ise õigusabi või soovitama seda teha juhtkonnal.	
CAAT-vahendite rakendamine alade haaval, edasist uurimist vajavate alade leidmiseks	Tuvastada suure väärtusega kreeditarved, saldod ja arved.	
	Teatada loodud arvete järjestuse lünkadest.	
	Tuvastada dubleeritud arved, krediidid ja laekumised.	
	Tuvastada arved, krediidid ja laekumised, mis pole õiges järjestuses või järjevahemikus.	
	Teatada loodud arvete järjestuse lünkadest.	
	Tuvastada allahindluste korrigeerimised.	
	Võtta kokku suured ilma ostutellimusteta arved tarnijalt.	
	Võrrelda kviitungi- või arvesummasid tellimuse- või lepingusummadega.	
	Tuvastada korduvad artikli- või sarjanumbrid.	
	Määrata käibe, hindade ja/või kulude protsentmuutused toodete või tarnijate lõikes.	
	Võrrelda kaubakviitungeid tarnete arvestusraamatuga ja teatada lahknevustest.	
	Leida kulumi tõttu allahinnatud artiklid, tuvastamaks maksumust ületava väärtusega varad	
	Arvutada käive kaubaklasside ja/või -artiklite lõikes.	
	Võrrelda kaubakviitungeid tarnete arvestusraamatuga ja teatada lahknevustest.	
	Tuvastada ebatavalised kohaletoimetuse aadressid.	
	Tuvastada suure kasumi- või hüvitusmääraga artiklid.	
	Eraldada välja kõik palgatšekid, kus summa ületab ettemääratu (töötaja kategooria järgi).	
	Tuvastada palgalehel kõik puhkuseta või haiguspäevadeta töötajad.	
	Tuvastada aegunud tellimused või osaliselt täidetud tellimused.	
	Tuvastada ostud igalt tarnijalt tellimisametnike haaval.	
	Võrrelda laoseise ja käibemäärasid.	
	Otsida jaotatud lepinguid (sama tarnija, sama päev).	
	Tuvastada tarnijate püsiregistris korduvad tarnijanumbrid.	
	Võrrelda tarnijate ja töötajate nimesid, aadresse ja telefoninumbreid.	
	Kontrollida krediitkaardisaldosid krediidilimiitidega võrreldes.	
	Tuvastada korduvad tagastustehingud.	
	Tuvastada tühistatud tehingud, millele ei järgne müüki.	
	Tuvastada artiklid, mis on müüdud turustushinnast odavamalt.	
	Arvutada müügiametniku tehtud tühistuste arv ja koguväärtus.	
	Määrata kauba päevane läbimüük kaupluste lõikes.	
	Võrrelda müügihindu kaupluste lõikes.	
	Võrrelda tooteid töökäskudes ja müügikorraldustes, netonõudluse analüüsimiseks.	
	Võrrelda üldplaanimiskorraldusi ajakavade täiustamise võimalustega.	
	Tuvastada mingile juba lõpetatud projektile määratud ressursid (tööjõud, materjalid).	
	Arvutada kaupade omahinna ja müügitulu suhe jms suhteid.	

	Koostada tarnijate rahanduslik kokkuvõte, millega toetada allahindluse läbirääkimisi.	
	Arvutada kustutamata laenude tagatise turuväärtus.	
	Korduvad nõuded samal perioodi kohta.	
	Tuvastada korduvad arved.	
	Tuvastada korduvad arvete aadressid.	
	Tuvastada laekumata tšekid.	
	Tuvastada kontodes tasaarveldamata ja pooleliolevad tehingud.	
	Tuvastada müügiametniku rahalised ülejäägid ja puudujäägid.	
	Kontrollida rahalisi saldosid (arvelduskrediiti).	
	Kontrollida, kas arvuti pääsu reguleerimise meetmed on asjakohased.	
	Kontrollida, kas arvutil töötluse erandid on käsitletud ja puuduvad tehingud on töödeldud.	
	Kontrollida arvuti korduskäituse analüüsi.	
	Kontrollida arvuti tõrgete analüüsi.	
	Kontrollida arvuti kasutamise analüüsi ning suutvuse plaanimist, analüüsi ja haldust.	

4.2 Korratuste näiteid

4.2.1 IS audiitor saab kahtlustamise põhjuste puudumisest mõningat kindlust, kuid ta ei tohiks oletada ei juhtkonna ebaausust ega ka vaieldamatut ausust. Nende protseduuride sooritamisel võib IS audiitor avastada asjaolusid, mis võivad viidata korratustele. Alljärgnevas on selliste olukordade näiteid.

4.2.2 Mitterahuldavate andmike või meetmete näiteid:

- halvad raamatupidamisdokumendid üldse,
- auditi asitõendid dokumentide võltsimise kohta;
- olulisi meetmeid ei hoita käigus;
- organisatsiooni dokumentide hävitamine enne kogu organisatsioonis nõutava säilitusaja lõppu.

4.2.3 Mitterahuldavate seletuste teemade näiteid:

- arvud, tendentsid või tulemused, mis ei vasta oodatavatele;
- ebatavalised üksused või vastavused või kahtlased kontod;
- hoiuleantud summade ebatavaline investeerimine;
- suured või ebatavalised tehingud, eriti perioodi lõpu lähedal ja eriti selliste firmade või pankadega, mis on organisatsiooniga seotud;
- õige perioodi registreerimine ja aruandlus;
- tehingute õige liigitamine;

- debitoorne võlg – müügitulu seletamatu kogunemine kontole aruandeperioodi lõpus (kaubakatteta müük);
- debitoorne võlg – debitoorse võla saldode seletamatu mahakandmine;
- kreditoorne võlg – (rahalise seisu parandamiseks) perioodi lõpule lükatud kulumaksed;
- laekumised – seletamatu laekumiste või hoiuste puudujääk.

4.2.4 Kahtlaste maksete näiteid:

- suured tasumaksed konsultantidele või nõustajaile, spetsifitseerimata teenuste eest;
- komisjoni- või teenustasud, mis näivad olevat liiga suured või ebatavaliselt väikesed, võrreldes tavalise tasuga selletaolise töö eest;
- suured maksed sularahas või pangaveksliga või välismaiste varifirmade kaudu või anonüümsete pangakontode kaudu;
- maksed kodu- või välismaistele riigiametnikele;
- üldine toetavate auditi asitõendite puudumine.

4.2.5 Muude kahtlaste asjaolude näiteid:

- volitamise probleeme puudutav kirjavahetus organisatsiooni ja ta reguleeriva asutuse vahel;
- organisatsiooni ja ta õigusnõustaja vaheline kirjavahetus, mille sisu on soovitus loobuda teatavast tegevuskäigust, kusjuures organisatsioon on seda soovitust ignoreerinud;
- juurdlus, mida sooritab riigiasutus või politsei;
- auditi asitõendid ametnike ja töötajate pillava elulaadi kohta.

5 ARUANDLUS

5.1 Olulised nõrkused

5.1.1 Auditi käigus tuvastatud olulistest sisejuhtimise nõrkustest tuleks viivitamatult teatada juhtkonnale (vt IS auditeerimise suunis G20 "Aruandlus") või mingile välisele asutusele, kui seda nõuavad õigusnormid.

5.1.2 Oluline nõrkus on olukord, kus IS audiitori arvates ei anna kehtestatud sisejuhtimisprotseduurid või nende täitmise tase mõistlikku kinnitust sellele, et olulised korratused välditakse või avastatakse.

5.1.3 Kui IS audiitoril on kahtlus, et võis aset leida suureriskiline korratus või et võisid aset leida ebaseaduslikud toimingud (ka siis, kui neid ei avastatud), peaks ta kõigepealt pidama nõu juhtkonnaga.

5.2 Auditi asitõendid

5.2.1 Olukorras, kus kahtlustatakse korratuse või ebaseadusliku toimingu asetleidmist või kus on asitõendeid selle kohta, et korratus või ebaseaduslik toiming on leidnud aset, tekib IS audiitoril kohustus uurida korratusi.

5.2.2 Sellisel juhul peaks IS audiitor kaaluma kirjaliku aruande esitamist asjakohastele pooltele, eraldi dokumendina (mitte auditiaruande osana), mis peaks esitama vähemalt alljärgneva.

- Hindamine sooritati auditiülesande tingimustele vastavas käsitlusalas, seega võisid muud korratused jääda tuvastamata.
- Aruanne ei järelda arvamust kogu sisejuhtimise kohta.
- Tuvastatud nõrkused on võetud arvesse auditiaruande jaoks.
- Juhtkonna kohus on rajada adekvaatne sisejuhtimine ja seirata seda.
- See aruanne on koostatud ainult informeerimiseks ja seda ei tuleks kasutada mingil muul eesmärgil.

6 JÕUSTUMISKUUPÄEV

6.1 See protseduur kehtib kõigi infosüsteemiauditite puhul, mis algavad 1. novembril 2003 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

LISA

Toetumine COBITile

Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ja arvestades COBITi teabekriteeriume. COBITi juhtimiseesmärk SH2 hõlmab juhtimise seiret ning korratuste ja ebaseaduslike toimingute vältimiseks ja avastamiseks oluliste sisejuhtimismeetmete õigeaegset kasutamist.

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs

1. TAUST

1.1 Seosed standarditega

1.1.1 Standard S6 „Audititöö sooritamine“ määrab: “IS auditi meeskonna üle peaks teostama järelevalvet, et anda mõistlik kinnitus auditi eesmärkide saavutamise ja kohaldatavate professionaalsete auditistandardite täitmise kohta.“

1.1.2 Standard S6 "Audititöö sooritamine" määrab: "Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega."

1.1.3 Suuniseid annab protseduur P3 „Sissetungi tuvastamise süsteemide (IDS) läbivaatus“.

1.1.4 Suuniseid annab suunis G25 „Virtuaalsete privaatvõrkude läbivaatus“.

1.2 Seosed COBITiga

1.2.1 COBITi raamstruktuur määrab: "Juhtkonna kohus on kaitsta kõiki ettevõtte varasid. Selle kohustuse täitmiseks ja oma ootuste saavutamiseks peab juhtkond rajama adekvaatse sisejuhtimise süsteemi."

1.2.2 COBITi "Juhtkonna suunised" annavad juhtkonnale suunatud raamstruktuuri pidevaks ja ennetavaks juhtimise enesehindamiseks, mis keskendub spetsiifiliselt

• soorituse mõõtmisele: kui hästi toetab IT-talitus tegevusalaseid nõudeid?

• IT juhtimise profileerimisele: millised IT-protsessid on tähtsad? Millised on juhtimise kriitilised edutegurid?

• teadlikkusele: millised on eesmärkide saavutamata jätmise riskid?

• mõõtlusele: mida teevad teised? Kuidas saab tulemusi mõõta ja võrrelda?

1.2.3 "Juhtkonna suunised" annavad näidismõõdustiku, mis võimaldab hinnata IT sooritust tegevusalases väljenduses. Kesksed sihiindikaatorid piiritlevad ja mõõdavad IT-protsesside tulemeid, kesksed sooritusse indikaatorid aga hindavad protsessi võimaldajate mõõtmise teel seda, kui hästi protsessi sooritatakse. Küpsusmudelid ja küpsusatribuudid võimaldavad suutlikkuse hindamisi ja mõõtlemist, aidates juhtkonnal mõõta juhtimise suutlikkust ning selgitada välja juhtimislünki ja täiustamise strateegiaid.

1.2.4 "Juhtkonna suuniseid" saab kasutada enesehindamise nõukodade toeks ja nendega saab toetada ka IT halduse süsteemi üheks osaks olevate pideva seire ja täiustamise protseduuride evitamist, mida sooritab juhtkond.

1.2.5 COBIT annab infosüsteemide halduse keskkonna tarbeks detailse juhtimismeetmete ja -meetodite kogumi. Konkreetse auditi käsitlusalale rakendatava kõige sobivama materjali valimine COBITist põhineb konkreetsete COBITi IT-protsesside valimisel ja COBITi teabekriteeriumide arvestamisel.

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

1.2.6 Teavet COBITi nende konkreetsete eesmärkide või protsesside kohta, mida tuleks arvestada selles juhises käsitletava ala läbivaatusel, annavad käesoleva suunise lisas olevad viited COBITile.

1.3 Protseduuri vajadus

1.3.1 See dokument on esmajärjekorras mõeldud IS sise- ja välisaudiitoritele, aga teda saavad kasutada ka teised IS turbe asjatundjad, kelle vastutada on infoturbe suutvus.

1.3.2 Tänapäevased ettevõtted on organiseeritud hulga tuumikprotsessidena, mis töötavad nõudluse ja pakkumise võrkudes. Peaaegu iga organisatsioon maailmas seisab vastakuti kasvava vajadusega toimivuse ja tõhususe järele (s.t kõrgemad kvaliteedinõuded toodetele ja teenustele, käibe kasvatamine, kulude vähendamine, uute toodete väljaarendamine); see on vajadus paremate, kiiremate ja odavamate protsesside järele. Neid üha keerukamaid töövõrke toetavad kättesaadavad sidetehnoloogiad (peamiselt Internet), mis võimaldavad ettevõtetel keskenduda tuumikpädevustele ja teha teistega koostööd klientidele lisaväärtuse pakkumiseks; seeläbi avab keerukus mitmeid teid ohtudele ja nõrkustele.

1.3.3 Vanade protsesside ümberkujundamise teevad võimalikuks uued sidekanalid. Need kanalid pakuvad uusi võimalusi mitmesuguste süsteemide ja võrkude ühendamiseks, tehes nad kättesaadavaks rohkematele inimestele ning võimaldades infovahetust ettevõtete ja nende protsesside vahel (nt e-hangete ja e-väljatöötuse puhul).

1.3.4 See dokument annab suuniseid IS audiitoritele, kellelt nõutakse üha enam perimeetri- ja sisemiste meetmete auditeerimist või läbivaatust, millega anda mõistlik kinnitus, et kõik välised ja sisemised ohud, sealhulgas potentsiaalsed süsteemi rikked, viiakse miinimumini, tuvastades ja parandades nõrkused, mis avastatakse läbistustesti ja nõrkuste analüüsi sooritamisel.

1.3.5 See protseduur ei asenda siseauditit, sealhulgas üleettevõttelist riskikaalutlust, sisemisi üldmeetmeid ega kõikide elutähtsate infrastruktuuride ja rakenduste auditeid, sealhulgas selliseid, mis mõjutavad raamatupidamisaruannet. Nõrkused mitte-elutähtsas infrastrukuuris ja rakenduste komponentides võivad avaldada olulist mõju elutähtsale infrastruktuurile ja rakenduste komponentidele, seetõttu tuleks ülesüsteemne revisjon viia lõpuni terviklikult ja mitte osahaaval.

2. LÄBISTUSTESTIMINE

2.1 Tutvustus ja plaanimine

2.1.1 Läbistustestimise ulatus määrab, kas eraldiseisvad toimingud tuleks sooritada etappidena või ühes jadas. IS audiitori sooritatav läbivaatus peaks algama formaalse ohtude kaalutlemisega, et teha kindlaks selliste organisatsiooni ähvardavate ohtude tõenäosus, mis tulenevad muuhulgas riistvara ja/või tarkvara riketest, personali põhjustatud turvariketest ja andmevargustest, või rünnakutest väljaspoolt.

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

2.1.2 Riskid, mis seonduvad volitamata pöördusega, varieeruvad alates rahalistest kahjudest, isiku-, äri- või poliitiliselt tundliku teabe paljastumisest ning mainekahjudest kuni kontrolli täieliku kadumiseni süsteemi üle. Volitamata juurdepääs inforessurssidele on spetsiifiline IS risk, mis realiseerumisel põhjustab kadusid süsteemi käideldavuses, andmete ja töötluse tervikluses ja teabe konfidentsiaalsuses.

2.1.3 Selle protseduuri eesmärk on katsetada meetmeid, mida tuleks rakendada kaitseks volitamata pöörduse vastu. Kuna volitamata pöörduseks kasutatavad meetodid on väga erinevad ja muutuvad üha keerulisemaks, on siinmääratletud protseduurid üldise loomuga ning kus võimalik, vajavad täiendamist uuritavale keskkonnale või -keskkondadele kohaste meetodite ja tööriistadega.

2.1.4 On märgatav vahe tegevustes, mida sooritab IS audiitor läbistustestimisel (lisaks juhtkonna heakskiidu omamisele) ja mida sooritab häkker. IS audiitor otsib testimise käigus nii palju potentsiaalseid nõrkusi kui testimisskript või -programm lubab, samas kui häkkerid otsivad tavaliselt vallutamiseks spetsiifilist nõrkust või -nõrkusi, eesmärgiga (tavaliselt) saavutada süsteemi üle kontroll või häirida tema tööd või käideldavust. On tõenäoline, et häkker jätkab järgmiste nõrkuste otsimist pärast esimese leidmist, et saada süsteemis täiendavaid privileege ja kaitsta end kasvanud avastusriski vastu. Seega kui läbistustestimist sooritaval IS audiitoril on suurem käsitlusala üldiste nõrkuste leidmiseks, siis häkker üritab tõenäoliselt vallutada iga avastatud nõrkust põhjalikumalt.

2.2 Protokolli pidamine

2.2.1 Protokollid peaks olema piisavalt üksikasjalikud, et toetada testimise leide ja järeldusi ning tagada järgmine:

• Kaitsta testi läbi viivat IS audiitorit süüdistuste eest ebaeetilistes või volitamata teguviisides

• Anda organisatsioonile üksikasjalik kirjeldus nõrkustest ning sellest, kuidas need avastati ja vallutati

• Luua tulevaste testimiste tarbeks revisjonipäevik, millega anda mõistlik kinnitus, et avastatud nõrkustele on pööratud tähelepanu.

• Tõendada, et suvaline sihikindel/tahtlik ja oskuslik ründaja toob kaasa volitamatu pääsu võimaluse ja riski.

3. LÄBISTUSTESTIMISE JA NÕRKUSTE KAALUTLEMISE LIIGID

3.1 Hindamise ulatus

3.1.1 On olemas mitmeid läbistustestide liike, mis asjaoludest sõltuvalt mõjutavad hindamise ulatust, rakendatavat metoodikat ja auditi kindlusastmeid.

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

3.1.2 Isik (asjakohasest IT-juhtkonnast), kes vastutab organisatsiooni kaitsmise eest, peaks kaalutlema mitmesuguseid alternatiive ning valima sellise, mis annab maksimaalse kindlusastme vähimate häiringutega, mis on ettevõttele aktsepteeritavad (tasuvusanalüüs).

3.1.3 Tuleks kokku leppida sooritatava läbistustestimise liik: kas sekkuv/süvatestimine või pindmine/mittesekkuv testimine.

4. VÄLINE LÄBISTUSTESTIMINE JA NÕRKUSTE KAALUTLEMINE

4.1 Internet

4.1.1 Interneti kaudu testimise eesmärk on rikkuda sihtvõrk. Selle testi sooritamiseks vajalik metoodika võimaldab süstemaatilist kontrollimist teadaolevate nõrkuste suhtes ja potentsiaalsete turvariskide otsimist. Harilikult kasutatakse metoodikat, mis sisaldab järgmisi protsesse:

• Info kogumine (luure)

• Võrgu inventuur

• Nõrkuste analüüs

• Vallutamine

• Tulemuste analüüs ja aruandlus

4.1.2 Jaotises 4.1.1 loetletud protsessidest on mitmeid variatsioone. Tavaliselt järgitakse siiski levinud, tüüpset ja objektiivset skripti, mis peaks tagama üksikasjaliku ja täpse sooritusviisi. Lisaks nõuavad uute nõrkuste keerukused ja uued vallutusviisid põhjalikku, varasemale infole toetuvat uurimist.

4.2 Sissehelistamine

4.2.1 Nn *war dialing* („sõjavalimine“) on häkkimismeetod, kus süstemaatiliselt helistatakse sihtvahemikus olevatele numbritele, et leida ootel modemeid. Pärast kõigi selliste modemite avastamist tehakse jõumeetodil katseid vaikeparoolidega või süstemaatilisi mõistatamiskatseid kasutajanime/parooli kombinatsiooni leidmiseks (vahel on vaja üksnes paroole), et saada volitamata juurdepääs.

4.2.2 Juurdepääs logimistekstile on igasugusele süsteemile juurdepääsuks elutähtis. Mõned süsteemid nõuavad üksnes parooli, mis võib olla tootja määratud vaikeparool või lihtsalt klahvi Enter vajutus.

4.2.3 Viletsa konfigureerimise puhul ei ilmu isegi logimistekst ning otsene juurdepääs antakse ilma igasuguse autentimismehhanismita.

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

5. SISEMINE LÄBISTUSTESTIMINE JA NÕRKUSTE KAALUTLEMINE

5.1 Eesmärk

5.1.1 Sisemise läbistustestimise eesmärk on kindlaks teha nõrkused seespool võrguperimeetrit. Sooritatav testimine on peaaegu võrreldav sellega, mille auditeerimiseks määratakse IS siseaudiitor, arvestades turvahuvi puudumisega seotud riski suurust, keerukust ja sellele määratud rahalisi vahendeid. Üldine eesmärk on avastada potentsiaalsed sisevõrgu nõrkused ja kehtestatud meetmete nõrkused, et hoida ära ja/või avastada nende väärkasutamisi, mida võivad sooritada häkkerid, kuritahtlikud töötajad või alltöövõtjad, kes võivad saada volitamatu juurdepääsu inforessurssidele või põhjustada süsteemi katkestuse või seiskumise.

5.1.2 Esimene etapp seondub teabe kogumisega, mis koosneb avaliku teabe otsimisest, otsimootori Google kasutamisest, maksimaalse teabe kogumisest ettevõtte, personali jne kohta, millega profileeritakse sihtmärk. Selle etapi tulemuseks võib olla näiteks töötajate elulookirjelduste/CVde hankimine, mis võib osutuda kasulikuks ründekohas kasutatavate tehnoloogiate mõistmisel.

5.1.2 Testimise esimene eesmärk on teha kindlaks sisevõrgu topoloogia või jälg, mis annab kaardi elutähtsatest pääsuradadest/punktidest ja seadmetest, sealhulgas nende IP-aadressivahemikest. See on võrgu avastamisjärk.

5.1.3 Kui elutähtsad punktid/seadmed on võrgus tuvastatud, on järgmine samm nende seadmete ründamine, kasutades mitmesugust liiki teadaolevaid nõrkusi süsteemis ja seadmete käitustarkvaras (nt UNIX, NT, Apache, Netscape ja IIS). Sellega on hõlmatud nõrkuste analüüsimise järk.

5.1.4 Kolmas ja viimane järk on vallutamine ja teavitamine.

6. FÜÜSILISE PÄÄSU REGULEERIMINE ANDMEKESKUSESSE JT TÖÖKOHTADESSE

6.1 Lubamatud pistikupesad

6.1.1 On elutähtis välja selgitada organisatsiooni hoonetesse (sealhulgas sideruumidesse ja andmekeskustesse) suubuvad ja neist väljuvad sidekanalid, et tuvastada potentsiaalsed meetodid andmeside vahelthaaramiseks, ärahoidmiseks või muutmiseks. Need juurdepääsukanalid peaks olema füüsiliselt kaitstud volitamata juurdepääsu eest ning tehtud kättesaamatuks ilma organisatsiooni eriloa ja teadmiseta ning ilma erivarustuseta.

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

7. SUHTLUSOSAVUSE TESTIMINE

7.1 Meetmete testimine

7.1.1 Suhtlusosavuse tehnikaid rakendatakse, et üritada hankida teavet perimeetervõrgu seadmete ja nende kaitsevahendite kohta (s.t IP-aadressivahemikud, tulemüürid ja vaikelüüsid), samuti potentsiaalsete sisemiste sihtmärkide kohta. Selle testi aluse piiritleb luurejärgus kogutav teave. Testi eesmärk on kaalutleda, kui lihtne on välja peilida elutähtsat teavet organisatsiooni siseressurssidest, personalilt/alltöövõtjatelt või teistelt, kes valdavad üksikasjalikku teavet organisatsiooni kohta, ilma et nad saaksid teadlikuks hangitud info tähtsusest. Eriti huvipakkuv on katse, kas organisatsiooni kasutajatugi abistab volitamata või tuvastamata kasutajat.

7.2 Telefonipääs

7.2.1 Esmase ja kõige olulisemana – mida rohkem teavet on testi sooritajal organisatsiooni, personali ja võrgu kohta, seda tõenäolisemalt õnnestub teavet välja peilida. Isik, kes testi sooritab, peaks kasutama skripti. Näiteks võib see isik esitleda ennast tehnilise tugiisikuna, kelle nimi hangiti varasema tugitelefonile helistamisega, otsides teavet ühenduvuse kohta ja seeläbi vajades võrguteavet. Sellised suhtlusosavuse katsed õnnestuvad tavaliselt siis, kui ühest allikast hangitud teavet kasutatakse kombinatsioonis teabega teisest, käesolevast allikast.

7.2.2 Test jätkub ning kasutades näites 7.2.1 toodud teavet, mis on hangitud tugitelefonilt, esitleb audiitor ennast telefonis organisatsiooni töötajana ning soovib parooli tühistamist/muutmist. Selliseid teste on parim läbi viia, kasutades organisatsiooni sisetelefoni, sest tugiisik/turvapersonal võib olla märksa rohkem nõus aktsepteerima teesklust ja anda küsitud teavet ilma üksikasjaliku autentimise või isikliku kinnituseta. Näideldes telefonis kannatamatut, pahurat või vihast klienti, samuti teised käitumisjooned (nt öeldes tugiisikule, et juurdepääsu on vaja ülemusele teabe edastamiseks, tema nime nimetamata) võivad õnnestumisele kaasa aidata.

7.2.3 Abiks on, kui testi sooritaja omab teeseldava töötaja kohta taustainfot nagu postiindeks, isikukood või ema neiupõlvenimi. Veelgi enam võib aidata töötajate elulookirjelduste/CVde hankimine, kasutades Interneti-otsingut või võõra värbaja lähenemist.

7.2.4 Veel üks lähenemine on konsultandi/audiitori teesklemine ja pöördumine IT-personali poole otse, ilma igasuguse tutvustuseta. Juhtkond peaks olema sellest teadlik ja sellega nõus, et hoida ära tarbetut tüli.

7.2.5 Sellest hoolimata on soovitatav, et kui testija takerdub, sest ei tea konfidentsiaalset firmaomast teavet, peaks ta end vabandama usutava õigustusega (nt halb enesetunne, ülemus vajab teda koheselt, pole hetkel aega vms). Iga hangitud infokild suurendab tõenäosust jõuda läbistusega õnnestunult elutähtsa infovarani.

7.2.6 Iga organisatsioon erineb teistest oma struktuurilt (nt tsentraliseeritud ja samas geograafilises piirkonnas või hoopis erineva juhtkonnaga ja laiali üle suure piirkonna), suuruselt (alates keskmisest, 500-800 töötajaga pangast kuni suure, üle 10 000 töötajaga finantshalduse ettevõtteni), võrgu keerukuselt ja turvateadlikkuselt (nt hästituntud organisatsioon või riigiasutus, mida sondeeritakse pidevalt portide skaneerimisega). Kõik testimisliigid on väärtuslikud, et hankida suhtlusosavuse teel väärtuslikku ja tundlikku teavet.

7.3 Jäätmete uurimine

7.3.1 Jäätmete äraveokohtade või prügikastide läbivaatus võib osutuda väärtuslikuks allikaks tundliku turvainfo ja üldise organisatsioonilise teabe leidmisel, millest võib kasu olla suhtlusosavuse katsetel. Elutähtsa teabe allikana tuleks kaaluda ka juurdepääsu korduvkasutatud paberi prügikastidele.

7.3.2 Organisatsiooni prügis sorimine võib tekitada kehavigastusi, kuna prügi võib sisaldada kõike alates teravatest objektidest kuni süstalde kuni ohtlike kemikaalideni. Läbistustestimise leping, kui testijaks on väliskonsultandid, peab sõnaselgelt lubama sellise testimisviisi.

7.4 Töölaua läbivaatus

7.4.1 Nagu eelpool mainitud, ei pruugi suhtlusosavuse kaudu hangitud teave olla kuigi asjakohane, välja arvatud siis, kui seda kasutatakse koos ülejäänud teabega, mis hangiti selles protseduuris kirjeldatud teiste testide kaudu. Üritades ära kasutada inimeste naiivsust või puudulikku väljaõpet firmaomase teabe kaitsmise osas, on kõige olulisem, et alati leidub keegi, kes paljastab infot, ning tavaliselt on üksnes aja küsimus, millal sellise inimesega ühendust võetakse.

8. TRAADITA TEHNOLOOGIA TAUST

8.1 Traadita tehnoloogiate taust ja seonduvad riskid

8.1.1 Koos andmete ja kõne edastamiseks kasutatava traadita tehnoloogia tulekuga on hakanud kaduma perimeeterseadmetega kehtestatavad hästituntud ja usaldatud meetmed. Kõrvaldatud on füüsilised turvameetmed, näiteks turvamehed, kaamerad ja lukud, mis olid tõhusad juhtmega võrkude ja andmeside kaitsmisel. Suured nõrkused tekivad, kui traadita tehnoloogiate kasutajad ei pööra tähelepanu järgmisele:

- Toetumine WEPile krüpteerimiseks
- Traadita võrkude eraldamata jätmine teistest võrkudest
- Kirjeldavate SSID- või AP-nimede kasutamine
- Püsiprogrammeeritavad MAC-aadressid

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

• Nõrk või olematu võtmehaldus

• Plinkimispaketid, mis pole blokeeritud või on „lubatud“

• Jagatud APd

• Vaikeparoolid/IP-aadressid

• Nõrkade WEP-võtmete vältimine

• DHCP kasutamine WLANides

• Kaitsmata lubamatud APd

8.1.2 Laialt on levinud riskid ja ohud, mis seonduvad rünnetega traadita võrkude vastu, sealhulgas:

• ründed, kus sõnumiliiklus haaratakse vahelt, analüüsitakse ja murtakse krüpteerimisvõtmed, nt initsialiseerimisvektori (IV) ründega;

• ressursivargus, kus saadakse Interneti-ühendus, mida seejärel kasutatakse teiste rünnakute (nt CRC-32) sooritamiseks;

• teenusetõkestus signaalihäirimise ning viirustest ja ussidest tuleneva ohu leviku tõttu.

8.1.3 Nagu teistegi tehnoloogialiikidega, on traadita tehnoloogia turvamisel suurim nõrkus „otse pakendist võetud“ ebaturvalised paigaldused, mitte tehnilised puudujäägid. Nõrgim lüli on tavaliselt inimfaktor.

9. VEEBIRAKENDUS

9.1 Käsi- ja automaattestimine

9.1.1 Veebirakenduse testimine sisaldab portaalisaidi käsi- ja automaattestimist väliskasutajana, ilma sisselogimisinfot omamata. See test täiendab välist läbistustestimist. Selle testimise eesmärk on jõuda arusaamisele, kuidas suhtlevad isikud süsteemiga tundlike andmete poole pöördumisel.

9.1.2 Täiendav testimine võib sisaldada portaalisaidi testimist sisekasutaja poolt, kasutades tavalist kasutajakontot. Selle testi eesmärk on teha kindlaks, kui lihtne on juurdepääs tundlikule teabele, mille pöördumiseks pole kasutajakontol voli (st privileegide eskaleerimine).

9.1.2 Nõrkuste avastamine ja vallutamine võib toimuda mitmesuguste tasuliste või avatud lähtekoodiga nõrkuste kaalutlemise tööriistadega.

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

10. SOOVITATAVAD PROTSEDUURID

	Soovitatavad läbistustestimise ja nõrkuste analüüsimise protseduurid	√
Plaanimine	Määratleda käsitlusala, tuginedes hindamise loomule, ajastusele ja ulatusele.	
	Kontrollida, et ükski test ei riku ühtegi spetsiifilist kohaliku või riikliku statuudiga seadust. Samuti peaks audiitor mõtlema organisatsioonilt allkirjastatud volituse hankimisele, mis lubaks läbistustestimise tööriistade ja meetodite rakendamist.	
	Uurida ja kasutada kättesaadavaid automaat-tööriistu, et sooritada läbistustestimine ja nõrkuste kaalutlemine. Sellised tööriistad tõstavad läbistustestimise tõhusust ja mõjusust.	
	Määratleda läbivaatuse ulatus, küsides järgmisi küsimusi: Kas IT-juhti ning arvutiturbe- ja IT-personali teavitatakse läbistustestimisest? Kas audititestimine keskendub turvameetmete nõrkuste avastamisele nende suhtes, kes pöörduvad info-infrastruktuuri poole Internetist ja sissehelistamise kaudu (välised) või organisatsiooni seest (sisemised)? Kui sügavale võrku ja infovarasse läbistustestimisega tungitakse? Näiteks kas testimine sooritatakse kuni tegeliku infovarade poole pöördumiseni välja või üksnes pääsukontrollipunktini (kus juurdepääsu infovaradele ei saavutata, kuid testimise alusel on piisavalt teavet, et see võiks juhtuda)? Kas test tuleb sekkuv või mittesekkuv? Millisel määral ja kui pikalt on lubatud üldine süsteemi degradeerumine testide läbiviimisel? Kas testi saaks sooritada töövälisel ajal, et vältida potentsiaalset konflikti, mille võib põhjustada elutähtis süsteemi seiskumine (nt nmap'i käivitamine tulemüüri vastu töövälisel ajal, nt pühapäeva hommikul, kui veebiteenuseid ei kasutata)?	
	Hankida juurdepääs (avalikule) nõrkuste andmebaasile, näiteks bugtraQ, packetstorm jt. Testija peaks veenduma, et kõik kasutatavad tööriistad on viidud ajakohaseks vastavalt uusimale nõrkuste andmebaasile.	
Nõutavad oskused	Tuleb omada piisavalt tehnilisi teadmisi ning võimet ära tunda ja/või avastada mitmesugust liiki ja variatsiooni turvanõrkusi ja puuke. Näiteks peaks isikul olema arusaam turvameetmetest, mida nõuavad läbistamine sissehelistamise kaudu, teenusetõkestus, paroolide murdmine, puhvrite ületäitumine ja traadita võrgud, samuti omama juurdepääsu ajakohase nõrkuste andmebaasi teenusele.	
	Tuleb omada põhjalikke teadmisi, kuidas töötavad mitmesugused tehnoloogiad, näiteks tulemüürid ja ruuterid, sissetungi tuvastamise süsteemid ja mitmesugust liiki autentimismehhanismid.	
	Tuleb omada praktilisi teadmisi rakenduste programmeerimisest, näiteks keeltes JAVA, Visual Basic ja C++.	
	Tuleb omada teadmisi mitmesugustest operatsioonisüsteemidest, näiteks UNIX, Linux, NT/2000, Windows ja OS/390 (või selle praegune suurarvuti-versioon).	
	Tuleb omada praktilisi teadmisi TCP/IP ja võrguprotokollide kohta.	
	Tuleb omada praktilisi teadmisi veebiserverite tarkvara kohta, sealhulgas Microsoft IIS ja Apache.	
	Tuleb omada teadmisi, kuidas kasutada valitud läbistustööriistu, et avastada puuke ja nõrkusi.	

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

	Tuleb omada teadmisi, kuidas avaldab sisesüsteemile mõju läbistamis- ja nõrkuste avastamise tööriistade rakendamine, sealhulgas NMAP, ISS, Whisker, Nikto, WebInspect, AppScan, ESM, Root, Nessus.	
Lepingud	Hoida alles kõik kirjed, sealhulgas spetsiifiline ja üksikasjalik klahvivajutuste ja suuliste vestluste logi kõikide läbistus- ja turvanõrkuste testimise käigus sooritatud tegevuste kohta. Need kirjed peaks olema piisavalt üksikasjalikud, et vajadusel saaks nende põhjal testi taasluua.	
	Hoida konfidentsiaalsetena kõik kirjed läbistustestimise kohta (sealhulgas ka tulemused), kuna nad on organisatsiooni omand. Kõik läbistus- ja nõrkuste testimise kirjed tuleks hoida organisatsiooni kontrolli all. Teste läbi viiv isik peaks organisatsiooniga allkirjastama vaikimis- ja eetilise käitumise lepingud, testi ja selle tulemuste ulatuse konfidentsiaalsuse osas.	
	Kui testi sooritab väliskonsultant, tuleb sõlmida leping organisatsiooni kaitseks. See leping peaks kehtestama teostatava töö piirid ja ulatuse ning tulemuste ja testiprotseduuride omaniku, samuti nõudma konsultantidelt konfidentsiaalsust ja eetilist käitumist. Lisaks peaks väliskonsultant pakkuma kindlustuse ja vastutuse (nn „hold harmless“) klausli, et leevenda riski juhuks, kui on toimunud teabe tahtmatu väljastamine.	
Ulatuse küsimused	Kas testimine koosneb juhtimiskeskkonna hindamisest, tuginedes info-infrastruktuuri läbistamisele seestpoolt või väljastpoolt võrguperimeetrit? Näiteks kui test koosneb tulemüüri reeglistiku hindamisest, tuginedes juurdepääsukatsele läbistada võrku Internetist, keskendub hindamine pääsumeetmete kindlakstegemisele väljastpoolt võrguperimeetrit. Perimeetri-meetmete testimise ulatust piiravad füüsilised ja loogilised turvameetmed, mis kaitsevad infovarasid organisatsioonivälise ohtude eest. Kord kui perimeetri turvameetmed on juba rikutud, tuleks teha otsus, kas jätkata testimist, et kindlaks teha siht-infosüsteemide turvameetmete piisavus. Nõrkuste testimine võib, vastupidi, keskenduda sisemise juhtimiskeskkonna hindamisele, et keelata seestpoolt lähtuv juurdepääs infovaradele.	
	Kas asjakohast juhtkonna tasandit, sealhulgas IT-turvet, on teavitatud läbistus- või nõrkuste testimisest? Kui testimise kohta tehakse formaalne teadaanne, võib sellega saavutada tiheda koostöö ja põhjalikuma hindamise. Sellele vastupidiselt võib etteteatamata testimine, mis põhineb tõelistel, volitamata pääsukatsetest tulenevatel ohtudel, paremini välja tuua tegelikud riskid ja juhtkonna reageeringu. Oluline on kaalutleda parimat stsenaariumit ja vajalikku kindlusastet.	
	Kas testi läbi viivatele isikutele on antud eelnevat teavet organisatsiooni kohta? Küsimus käib kokku sellega, kas juhtkonda on teavitatud testimise loomust ja ulatusest. Mõnikord teavitatakse testist üksnes tippjuhti või IT-juhti ning personal jäetakse teavitamata. Sellest hoolimata, kui teave (nt võrgu topoloogia) on antud ja testija seda kasutab, saab võimalikuks üksikasjalikum sihtsüsteemide ja -protsesside uurimine, mille tulemus võib olla riskide ja nõrkuste parem kindlakstegemine. Siseinfo andmine võib siiski lõppeda raskustega nõrkuste ulatusest ja nende vallutamise tõenäosusest arusaamisel. Lisaks eelnevale tuleks testida ka IP-vahemikke, kui juhtkond need annab.	

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

Läbistus-testimine Interneti kaudu	Võrguinventuuril saadakse järgmine teave: võrguressursid ja -jaosed; kasutajanimed, sh vaikimisi („otse karbist“) kaasasolevad riist- ja tarkvaramüüjate kasutajanimed, kasutajanimed ja neile vastavad grupid ning rakendused ja logimistekstid. Tuleks mõelda järgmistele sammudele: • Teha kindlaks domeeninimi, IP-aadressivahemik ja ülejäänud elutähtis teave. Tavaliselt kasutatakse selleks päringut „who is“, mis üldjuhul annab sihtvõrgu aadressi (st nimeserverid ja IP-aadresside vastendused), halduskontaktid ja arvelduskontaktid. Isik, kes sooritab „who is“-päringu, peaks andma mõistliku kinnituse, et kätte saadakse kõik kirjed, mitte ainult esimesed 50, milleks võib olla vajalik täpsustada päringus esinevaid isiku- või ettevõttenimesid. • Teha kindlaks organisatsioonile kuuluda võivad IP-aadressivahemikud. Üldjuhul esitatakse selleks päring mõnele Interneti-registrile nagu ARIN, RIP, APNIC või LACNIC. •Välja selgitada välised e-maili serverid, kogudes DNS-serveritest MX-kirjete andmeid. •Üritada tsooniedastust kõikide DNS-serveritena (sh varuserverid) tuvastatud süsteemide vahel, et hankida võrgu IP-aadresside loend ja arvutite hostinimed. Tsooniedastus küsib täieliku nimekirja hostinimede ja IP-aadresside vastendustest, mida hoitakse DNSis selle domeeni kohta. Lisaks on võimalik utiliidi „nslookup“ abil, mida toetavad nii UNIX kui ka Windows, sooritada tsooniedastus, kasutades DNS-serverit, mis on huvipakkuva domeeni jaoks autoriteetne. Lisaks võivad arvutite hostinimed viidata nende otstarbele (nt meiliserver ja tulemüür), mis on järjekordne elutähtis infokild. Uute tehnoloogiatega kaob võimalus tsooniedastuseks ilma algatava seadmeta. • Teha kindlaks, kas organisatsioon on oma domeeninime talituse üle andnud Interneti teenusetarnijale (ISP). Juhtudel kus see talitus on väljasttellitud, on soovitatav, et läbistustestimise tingimused sätestaks selgelt, kas hostitud süsteem jääb testimise käsitlusalasse. • Teavitada võrgupersonali, et käimas võib olla läbistustestimine, sest tsooniedastust saab avastada. • Kasutada võrgu pingimist ICMP ping või TCP ping (täieliku või pooliku TCP kätlusega) abil, et teha kindlaks, millised IP-aadressidele vastavad arvutid on “elus” või töös. Ehkki see samm võib anda elutähtsat teavet selle kohta, millised seadmed on aktiivsed, on võimalik, et perimeetri turvaseadmed või tulemüürid võivad hostile suunatud ICMP-liikluse kõrvale heita. Liiklus võidakse filtreerida või kõrvale heita vastusega, mis osutab seadme mittetöötamisele, kuigi tegelikult seade töötab. Avastamise vältimiseks on soovitatav segada pingitavate IP-aadresside järjekord ning varieerida NMAPi. NMAP on populaarne tööriist UNIX-süsteemide jaoks ning utiliite Pinger ja WS_Ping ProPack kasutatakse Windows-keskkondades võrgu pingimiseks. • Kasutada meetodit “traceroute”, et teha kindlaks pakettide teed pingimise sihtmärgini. Seejärel saab teid jälitada töötavate sihthostideni, mis avastati võrgu pingimisega, et tuletada ligikaudne kaart organisatsiooni arhitektuuri topoloogia kohta. Kaks tavalist tööriista on “traceroute” ja “tracert”, mida saab kasutada nii UNIXi- kui ka Windowsi-põhistes operatsioonisüsteemides. Selle meetodi otstarve on avastada harilikud ja ebaharilikud “hüpped” enne sihtmärgini jõudmist, mis võivad osutada asjadele nagu tulemüürid, filtreerivad ruuterid või muud lüüsid, koormust tasakaalustavad seadmed või veebiliikluse ümbersuunajad Võrgusegmentidel võivad olla mitmed ühendused Internetiga, ilma et võrgugrupp seda teaks. Kuid kui sellised vähelevinud teed jäetakse kontrollimata, võivad need viia võrguriketeni. • Saata “võlts”-meilisõnumeid organisatsiooni domeenidele, et üritada tagastatavat meili kätte saada. Tagastatud meilide päis tuleb läbi vaadata, et avastada võimalikke võrguteid.	

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

	Nõrkuste analüüsi sooritamiseks tuleb teha järgmist: • Kaalutleda võimalikke ründemeetodeid nõrkuste tuvastamise alusel. Selleks tuleb uurida kõiki sihtvõrgust leitud arvuteid, et avastada kõik lahtised pordid, operatsioonisüsteemid, rakendused ja nende hostid (sealhulgas versiooninumber, paigatase ja/või paigakomplekt). Lisaks tuleb seda teavet võrrelda Internetis olevate nõrkuste andmebaasidega, et teha kindlaks, millised asjakohased nõrkused ja vallutused võivad olla rakendatavad sihtvõrgule. • Tuvastada sihthostides käitatava operatsioonisüsteemi (OS) liik. Võrguinventuuri etapis tuvastatud sihthostide puhul saab kasutada utiliiti NMAP, et OSi liik kindlaks teha. Käitatava OSi liik on elutähtis ennustamiseks, millised teenused on kättesaadavad ning seejärel selleks, et kohandada selle pordi kaudu antava teenuse sihtanalüüsi, mis teostamisel teeb kindlaks konkreetsete nõrkuste olemasolu. Ühes selle sammuga tuleb hankida ajakohane loetelu käitatava OSi nõrkustest, otsides nende nõrkuste kohta detailandmeid OSi müüja veebisaidist ja nõrkuste andmebaasidest. • Tuleb hankida luba "töötavate" sihthostide portide sondeerimiseks. Kui turvagrupp on teadlik läbistustestimisest, võib vaja olla sondeerida kõiki võimalikke porte (1-65535). Portide loend peaks sisaldama rakendusi, millel on teadaolevad nõrkused. Uuritavad pordid peaks olema seotud nõrkuste või infokogumisega. Näiteks kasutatakse tihti ära protokollide FTP, Telnet ja RealSecure porte (21, 23 ja 2998), et üritada nõrkuste vallutamist. Tavaline tööriist on NMAP, mida saab programmeerida sooritama nende sihthostide portide sondeerimist, mis võrgu pingimise põhjal olid "elus". Ilma portide omanikult saadud otsese loata on portide sondeerimine selgelt ebaeetiline. Portide sondeerimine, nagu ka mitmed teised nõrkustetestid, on tehnika, mida võivad kasutada häkkerid ning mis peaks hoiatama turvagruppi võimalikust läbistuskatsest. • Sooritada rakenduste inventuur, et tuvastada portidele määratud teenused (rakendused). Lisaks portide sondeerimisele toimub pordile määratud teenuste (rakenduste) täpne tuvastamine, mida nimetatakse rakenduste inventuuriks. Teadmine, milliseid rakendusi sihthostid käitavad, aitab palju kaasa nõrkuste analüüsi teostamisele. Tavaliselt käitatakse rakendusi läbi Interneti. Tuleb leida loetelu nende rakenduste teadaolevatest nõrkustest ja vallutustest, mis on tihti võimalik saada müüjatelt endilt või nõrkuste andmebaasidest. Rakenduste inventuur sisaldab ka logimisteksti püüki, mis võib olla abiks töötavate rakenduste tuvastamisel. Seda saab teha paljude rakendustega, sealhulgas Netcat, mis töötab nii UNIXi kui ka Windowsi käsurealt; Telnet, ja What's Running, mis on graafilise kasutajaliidesega tööriist Windowsile. Levinud infoallikateks süsteemi- ja rakendustarkvara nõrkuste ja vallutuste kohta on näiteks Bugtraq listid, Packetstorm ja SecurityFocus. • Käitada tasulisi või avatud lähtekoodiga võrgunõrkuste kaalutlemise tööriistu, et kontrollida tulemusi. Populaarsete tööriistade hulgas on Nessus, ISS Internet Scanner, Foundstone FoundScan, eEye Retina Scanner ja GFI LANguard. Nõrkuste analüüsi käigus leitud nõrkused tuleb vallutada, et üritada juurdepääsu sihtsüsteemile juurkasutaja või süsteemiülema tasemel, või juurdepääsu mõnele teisele usaldatud kasutajakontole, vastavalt järgnevale:	

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

	• Saades nõrkuste analüüsil tuvastatud pääsupunktide kaudu juurdepääsu sihtsüsteemi käsureale, tuleb dokumenteerida kogu asjakohane teave, sealhulgas järgmine: hosti ja kataloogi või jaose nimi, kuhu saadi juurdepääs; juurdepääsu kuupäev, kellaaeg ja tase; ning viimaks turvaauk või –augud, mida vallutati juurdepääsu saamiseks. • Sooritada rikutud hostist rünnakuid teiste süsteemide vastu võrgus. Kui võimalik, paigaldatakse rikutud hostidesse tööriistakomplekt, mis on kohandatud teiste sihtmärgiks võetud arvutite operatsioonisüsteemidele. Tööriistakomplekt võib sisaldada rakendusi nagu Netcat, paroolimurdjaid, kaugjuhtimistarkvara, nuuskureid ja avastustööriistu, mida saab käivitada käsurealt. Selles etapis liitub Interneti kaudu (s.t väline) läbistamismeetod sisemiste testimismeetoditega, mida kirjeldab jaotis 5. • Teavitada organisatsiooni, kui pääsutase on saavutatud, tehes seega võimalikuks ohtlike viiruste paigaldamise, mis võib lõppeda süsteemi seiskumisega.	
Sissehelistamisega läbistustestimine	Saavutada läbistamine, helistades sisse telefoniliini kaudu, mis kuulab sissetulevaid ühendusi, ja logida end hostarvutisse. Otsitavate nõrkuste seas võib olla näiteks järgmisi: • Arvutite külge ühendatud modemid, näiteks marsruuterid, mida riist- ja tarkvara müüjad kasutavad arvuti hooldamiseks (nt paikade installeerimiseks). • Lubamatud modemid, mis on ühendatud aktiivselt kuulavate kasutajate töölaudadega. • Modemid, kuhu on installeeritud kaughalduse tööriistad, näiteks PCAnywhere. • Lubatud, kuid ebaturvaliselt seadistatud modemid.	
	Koguda kõnede tegemiseks kasutatud telefoninumbrid. Allikate seas on telefoniraamatud, kataloogid võrgus, reklaammaterjalid ettevõtte kohta ja trükised. Sisemised telefonikataloogid võivad olla eriti väärtuslikud, kui need on kättesaadavad. Need võivad põhineda teatud vahemikku jääval telefoninumbrite plokil või plokkidel, mis võivad olla geograafiliselt määratud: • Tuleb leida, kus asub sihtorganisatsioon füüsiliselt, mis määrab ära tema postiindeksi. • Tuleb üritada nende numbrite organisatsioonist sõltumatut hankimist, et teha kindlaks selle keerukus. Selleks võib vaja minna teatud tasemel suhtlusosavust.	
	Tuvastada kuulavad modemid, helistades suvalises järjekorras igale sihtvahemikku jäävale numbrile. Kasutada saab nn sõjavalimise tarkvara, millega helistada ning salvestada vastused, et teha kindlaks kuulavad modemid.	
	Pärast kuulava modemi avastamist tuleb saada volitamata juurdepääs, tehes jõumeetodil katseid vaikeparoolidega või tõenäolisi oletusi kasutajanime/parooli kombinatsiooni leidmiseks. Nn sõjahelistamise tarkvara saab panna üritama sisselogimispääsu, kasutades suurimat võimalikku loetelu ja/või valikulist loendit vaike-kasutajanimedest ja paroolidest. Valikuline vaikeloend võib sisaldada ka tõenäolisi oletusi kasutajanime/parooli paari kohta. Näiteks Cisco marsruuteri puhul võib kasutajanime/parooli paar olla Cisco/Cisco või enable/Cisco -- või kui küsitakse ainult parooli, siis võib proovida c, cc, cisco ja Cisco router. Proovida tuleks ka müüja loodud vaike-kasutajanime ja parooli, kuna väga tihti jäetakse need vahetamata või blokeerimata.	
	Teha kindlaks, kas demilitariseeritud tsooni (DMZ) veebiseadmetesse on installeeritud nuuskureid või klahvivajutuste logijaid, mis püüavad kasutajanimesid ja paroole.	
	Tuleb arvesse võtta, kas tarkvara PCAnywhere kasutatakse seadistatuna lubama autentimata ühendusi juhul, kui helistav klient kasutab samuti PCAnywhere'i.	

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

Sisemine läbistus-testimine	Sooritada võrgu avastamise test, tehes järgmised sammud: • Sooritada võrgu pingimine, et tuvastada töötavad hostid. Levinud tööriistade hulgas on NMAP Pinger, NetScan tööriistad ja WS_Ping ProPack tööriistad. • Kui võimalik, tuleks välise läbistustestiga rikutud hostidesse installeerida nuuskurid, mis selgitavad välja ARP-tabelid, SNMP andmed ja marsruutimisinfo. • Üritada tsooniedastust, et saada teada sisemised IP-aadressid ja arvutite nimed, mis võivad osutada hosti otstarbele. • Üritada marsruudi jälitamist (utiliidiga traceroute), et täpsustada elutähtsaks peetavate sihthostide loendit. • Tuleb ära arvata vaikeparool või kas parooliks on pandud sõna "public" või "private", et hankida ründe algatamiseks SNMP-teavet, mis sisaldab marsruutimistabeleid, protokolle, vealogisid ning muid andmeid süsteemi ja võrgu kohta. Tuleb üritada ka sagedamini kasutatavate vaikeparoolide (nt Cisco, {firmanimi}, router, switch, network) äraarvamist. • Pärast ülaloleva täideviimist tuleb saada turvagrupilt volitus, et installeerida hostipõhised automaatsed avastustööriistad, mis annavad nõrkuste täisnimekirja. Levinud tööriistade seas on Enterprise Security Manager (ESM), ISS jt.	
	Sooritada nõrkuse analüüs, tehes järgmised sammud: • Käivitada sihthostides portide sondeerimise ja logimisteksti püügi rakendused, et tuvastada aktiivsed teenused. See on võrreldav välise läbistustestimisega. Seda sammu saab teha ühenduses võrgu pingimisega NMAPi abil. • Kontrollida vallutuste leidmiseks iga süsteemitarkvara liiki konkreetsete teadaolevate nõrkuste suhtes, ja samuti ka avatud porte. Näiteks tuleks testida teadaolevaid anonüümse FTP nõrkusi, et teha kindlaks, kas esmalt saaks neid nõrkusi ära kasutada vallutusskriptiga ning seejärel paigaldada utiliiti Netcat sisaldav juurvarje *(rootkit)*, millega avada teatud etapis käsurida. Eksisteerib arvukalt teadaolevaid nõrkusi, mille hulk kasvab pidevalt. • Tuleb hankida volitus turvagrupilt, et paigaldada automaatsed avastustööriistad, mis annavad nõrkuste täisnimekirja. Selliste tööriistade hulgas on Cybercop, Enterprise Security Manager (ESM) ja Internet Security Scanner (ISS) ning Nessus. • Tekitada tabel IP-aadressidest, hostinimedest, süsteemitarkvara liikidest (nt UNIX ja NT), avatud portidest ning rakendustest (nt Netscape, IIS ja Apache).	
	Sooritada vallutamine ja teavitamine, tehes järgmised sammud: • Teha kindlaks ründetase, mida organisatsioon sooviks ja heaks kiidaks. • Teha kindlaks ründetase, võttes aluseks kas avatud portidele ning avastus- ja analüüsietappides piiritletud sihthostidele hangitud pääsutaseme või organisatsioonilt saadud info. Näiteks kui sihthost on UNIXi-põhine, siis pärast sellele seadmele juurdepääsu saamist võiks proovida tema paroolifaili murda. Kui ründaja suudab avastamatuks jäädes hankida juurdepääsu teistele seadmetele ja väärtuslikele firmaandmetele, on läbistus täiesti õnnestunud. • Teavitada organisatsiooni, kui pääsutase on saavutatud, tehes seega võimalikuks ohtlike viiruste, juurvarjete või teiste tööriistade või tarkvara paigaldamise, mis võib lõppeda süsteemi seiskumisega, või et näidata, kuidas ründaja saab avastamatuks jäädes säilitada volitamata juurdepääsu. • Dokumenteerida kõik märgatud nõrkused ja anda need pärast läbistustesti/nõrkuste analüüsi lõppemist organisatsioonile kohese uue läbivaatuse jaoks.	

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

Füüsilised pääsu-meetmed	Otsida lubamatuid pistikupesasid, mida saab vallutada. Tuleb tuvastada pöördusteed, mis suubuvad tööaladele ja andmekeskusesse ning väljuvad neist. Pöördusteed tuleks kaevata maasse või tühistada ning need ei peaks olema juurdepääsetavad laiemale avalikkusele. Üritada kindlaks teha kaableid lagedes või suletud ruumides, kus võib ilmneda volitamatu pealtkuulamine, kuigi see ei pruugi alati olla võimalik, eriti arvestades fiiberoptilise kaabli kasutamist.	
	Kui võrgule on saadud füüsiline juurdepääs, sooritada jõumeetodil ja valikuline pöördus vaike-kasutajanimede poole.	
	Saada füüsiline juurdepääs ja alustada suhtlusosavuse kasutamist nagu määratletud selle protseduuri jaotises 7: Ilma end personalina identifitseerimata tuleks üritada takistamatu juurdepääsu hankimist. Organisatsiooni aladel, kus rakendatakse füüsilist kaitset mehhaanilise, elektroonilise või füüsilise tõkise abil, saab seda testi läbi viia mitmel viisil, sealhulgas legitiimse töötaja kannul sisenedes või meldides end sisse ilma saatjata ning kõndides otse andmekeskusesse või ettevõtte äriruumidesse. • Tüüpne äritava peaks piirama otsest takistamatut juurdepääsu kõigisse äriruumidesse. • Konsultatsioonileping või testi läbi viiv siseaudiitor peaks selgesõnaliselt nõudma käesolevat hindamist. • Tuleks läbi viia andmekeskuse revisjon, et hinnata kõiki füüsilisi turvameetmeid andmekeskuses ja teistes tööalades.	
	Ehitada tara ümber andmekeskuse, et takistada sissetungijatel edastussignaalide püüdmist.	
Suhtlusosavuse testimine	Kontrollida meetmeid, mis on kehtestatud, et ära hoida suhtlusosavust või loogilistest turvameetmetest möödahiilimist, teeseldes sisetelefonilt helistades inimest, kes nõuab ärivajadustel äärmiselt tundlikku teavet või juurdepääsu põhilistele arvutusteenustele.	
	Kui läbistustestimist viivad läbi välised konsultandid, lubada läbistustestimise lepingus selgesõnaliselt jäätmete äraveokohtade kontrollimist.	
	Tuleb läbi vaadata konfidentsiaalsuspoliitikad ja –tavad, et teha kindlaks, kelle vastutada on firmainfot sisaldavate püsikoopiate kõrvaldamine ja purustamine. Andmete kõrvaldamisele kehtestatud turvameetmed on elutähtsad.	
	Tuleb läbi vaadata meetmed, mis on kehtestatud tundlikke andmeid sisaldava magnetmeedia kõrvaldamisele.	
	Juhul kui saadakse füüsiline ligipääs töökohale, tuleb läbi vaadata kõikide töötajate töökohad ning printerikorvid, et leida firmaomast teavet, näiteks kasutajanimesid, arvutite nimesid ja teavet teiste töötajate kohta. Kleepmärkmed ja tööplaanid võivad olla olulise teabe allikaks.	
	Hankida elutähtsate alade ehitusjoonised ja korruseplaanid. Tööalad nagu vara- ja väljamakseosakonnad ning juhtide ametiruumid on esmased sihtmärgid.	
	Teha kindlaks, kas iga lauaarvuti kasutab ekraanisäästjat ning töölauad on lukustatud.	
	Tuleb anda mõistlik kinnitus, et töö ulatus ei riku ühtegi seadust.	
Traadita võrgud	Tuleb leida traadita võrgud ning kanda need tänavakaardile või loodusgeograafilisele maa-ala kaardile. Tööriistade hulgas, mida on vaja traadita võrgu läbistustestimiseks, võivad olla sülearvuti/pihuarvuti, võrguadapter traadita võrgule (ORiNOCO või Lucent PC, Card Dell TrueMobile 1150, Avaya Wireless PC Card, Compaq WL110, Enterasys Roamabout Elsa Airlancer MC-11), tasuta tarkvara ning antenn ja GPS. Üks meetod traadita võrkude leidmiseks on nn *war driving* ("sõjasõit"). Selleks tehakse kindlaks majakas ja levisaade. Sõjasõitu kasutatakse traadita sagedusribast signaali püüdmiseks ja kaardistamiseks.	

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

	Tuleb murda WEP-võtmed (Wired Equivalent Privacy), kasutades automaatvahendeid nagu WEPCrack ja AirSnort. Murdmismeetoditena kasutatakse IV kollisioone ja nõrga võtmega paketihõivet.	
	Tuleb nuuskida ja analüüsida võrguliiklust, et teha kindlaks paketiedastuste arv, võrgu SSID jne. Selleks on mitmeid automaatvahendeid, näiteks PrismDump, Iris, AiroPeek ja Sniffer Wireless.	
	Pärast võtme teadasaamist tuleb pakett uuesti kokku panna, millega on läbistustest lõppenud. Kõik märgatud probleemid tuleb dokumenteerida juhtkonnale läbivaatamiseks. Enne seda testi oleks hea konsulteerida juristidega, kelle ametialane tegevus toimub vastavates riikides ning, kus vajalik, kohalikul ja sellest kõrgemal tasandil. Sellega tuleb saada mõistlik kinnitus, et selle testi läbiviimine ei riku ühtegi õigusakti, kuna testimisel püütakse kinni infopakette ka teistelt, soovimatutelt sihtmärkidelt.	
Veebirakendus	Riski piiritlemiseks tuleb analüüsida veebirakendused ja -keskkond, käies esmalt läbi veebilehtede, et koguda teavet, sealhulgas kõikide lehtede kaardistus ja üldine arusaam kogu funktsionaalsusest. Täpsemalt tuleb käsitsi sirvida rakendust, kasutades salvestavat proksit (nt webproxy, ebsleuth), et leida varjatud andmeid ja avastada vormide nõrkusi. Ühes selle uuringuga tuleb teha järgmist: • Läbi vaadata SSL/TLS-šifrite kogu, et teha kindlaks kooskõla poliitikate või tööstuse tüüptavadega. • Analüüsida seansijälitust, sealhulgas selle mehhanismi ja seansi ID-d. • Tuleb välja selgitada kasutatavad autentimismeetodid, sealhulgas kliendisertifikaatide kasutamine, sertifikaatide kontrollimine ja tühistamine, krüpteerimise või HTTP-lihtautentimise kasutamine ning SSL-i tarvitusele võtmine. • Tuleb välja selgitada sisse- ja väljalogimise mehhanismid (puhverdusvastased meetodid ja seansi aegumine põhjustavad automaatset väljalogimist). • Tuleb välja selgitada kõik kasutajasisendi kohad, salvestades kõik vormielemendid, täpsemalt: □Proovida SQL-süstimist □Üritada kontrolli saamiseks puhvri ületäitmist □Proovida murdskriptimist (XSS) □Proovida erisümboleid (püstkriipsud, reavahetused jne) □Arvsisendis proovida nulli, negatiivset väärtust, väga suurt väärtust □Salvestada kõik sõnaohtrad veateated. Lisaks testida iga sisendina kasutatavat HTTP-päist nagu Cookie, Referrer, Host, User-agent. □Salvestada kasutatav permutatsioonide nimekiri □Testida URLis sisalduvat kasutajasisendit POST-päringuga. • Läbi vaadata veebirakenduse väljund peidetud sisu või infolekke leidmiseks. • Otsida kliendipoolsest lähtekoodist (META-sildid, kommentaarid) ebavajalikku teavet. • Teha kindlaks, kas HTTP-vastus serverilt sisaldab ebavajalikku teavet ("Server:", prefiksiga "X-" algavad väljad). • Teha kindlaks, kas Java-aplettid ja muud sarnased on dekompileeritud. • Välja otsida ja läbi vaadata iga teadaoleva kataloogi robots.txt	

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

Veebirakendus (jätkub)	• Läbi vaadata seansitunnuste turvameetmed, testides muuhulgas järgmist: □Teha kindlaks, kas seansitunnused on juhuslikud, ei seondu kasutajainfoga, on piisavalt pikad jõuründe vältimiseks, on aeguvad, on edastatud üle turvatud tee; ning on kehtestatud meetmed nende manipuleerimise vältimiseks ja mehhanismid selle avastamiseks. □Teha kindlaks, et seansitunnustega prääniкud on märgistusega "turvaline" (krüpteeritud), mittepersistentsed (ei säilitata kõvakettal), mõistlikult piiratud domeeni ja rajaga ning, kui see on asjakohane, digitaalselt allkirjastatud. □Kontrollida, et seansitunnusega URLid saadetakse krüpteeritult, näiteks SSL-iga. • Tuleb läbi vaadata sisselogimisele kehtestatud turvameetmed, sealhulgas: Hoiatustekst ja tõrketeated, mis hoiatavad volitamata häkkimiskatse eest. Kui tehakse sisselogimiskatse vale kasutajanime või parooliga, siis üldine teade ei anna täpset teavet, kumb neist oli vale. Esmase, mandaati sisaldava sisselogimise krüpteerimine Taimaut pärast teatud inaktiivsusperioodi, et vältida poolavatud seansse. Lukustusmehhanism vigaste sisselogimiskatsete puhuks, et vähendada jõurünnakute ohtu. Lukustusmehhanism ei too kaasa teenusetõkestust olulise arvu peatatud kasutajakontode suhtes, vaid pigem annab ründest märku, tuues kaasa eskaleerumisprotsessi. • Teha kindlaks, kas kogu edastatud info on krüpteeritud, näiteks veendudes, et veebibrauser näitab tabaluku ikooni. Teha kindlaks, kas kõik saadetud ja vastu võetud lehed on krüpteeritud. Ühiselt läbi vaadata uuringu hindamise tulemused ja portaali testimissammude tulemused, et teha kindlaks nõrkused, mida on võimalik vallutada tundlikule teabele juurdepääsu saamiseks, kus vallutajaks võib olla nii väline kasutaja, kellel pole teavet süsteemi kohta ega kasutajakontot, kui ka sisekasutaja, kellel on teadmised süsteemi kohta ja kasutajakonto. Märkus: Kuna aja möödudes avastatakse arvukalt porti 80 kasutavaid nõrkusi, on soovitatav, et selle testi läbiviijad omaksid ajakohast teavet, mis ületab selle, mis on määratletud mitmesugustes uurimisdokumentides, lühiülevaadetes ja veebilehtedel. Lisaks tuleks läbi viia sari veebiserverite revisjoniteste, sealhulgas tüüpne pääsuloendite ja TCP/IP nõrkuste hindamine, mis on kirjeldatud selle protseduuri teistes osades.	

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

Veebirakendus (jätkub)	Käitada tasulisi või avatud lähtekoodiga rakenduste nõrkuse kaalutlemise tööriistu, et kontrollida tulemusi. Populaarsete tööriistade seas on Nikto, WebInspect, ScanDo ja AppScan. Eksisteerib arvukalt potentsiaalseid nõrkusi, mida saab avastada ülalkirjeldatud testidega. Sellele vastavalt on teine etapp potentsiaalsete nõrkuste vallutamine, mis hõlmab muuhulgas järgmist: • Muuta prääniкute sisu (nt muuta rakendusele URLi kaudu edastatavaid parameetreid), mis annab juurdepääsu tundlikule teabele või võimaldab maskeeruda mõneks teiseks kasutajaks. • Muuta JavaScript'i rakenduse sees või rakenduse vormide peidetud vormiväljadel; kasutada parameetrite manipuleerimist, SQL-süstimist (sisestada rakendusse mitte ettenähtud SQL-lähtekoodi), murdskriptimist (sisestada käivitatavaid käske veebisaidi puhvritesse). • Sisestada koodi tekstiväljadesse, et haarata rakenduse üle kontroll. • Pöörduda jõurünnet kasutades otse veebilehe poole, mis harilikult on kättesaadav üksnes läbi autentimise. • Koguda kasutajanimesid kohtades, kuhu on sisestatud valed paroolid ning sooridada nende vastu sõnastikurünne. • Otse vallutada tagauksi ja silumisvõimalusi, sealhulgas käivitada URLides silumissüntaksit (nt leiab nõrkuste loetelu mitmesugustest veebisaitidest, sealhulgas CERT, ja müüjate saitidest nagu näiteks *www.nstalker.com*). • Vallutada mingeid konfigureerimisvigu kolmanda poole rakendustes, näiteks veebi- või andmebaasiserverites. Tuleks teha konkreetseid katseid vallutada teadaolevaid nõrkusi veebiserveri vaikekonfiguratsioonis. • Sisestada skriptimiskeelte lausungeid tekstilahtritesse, mida näevad teised kasutajad. • Anda rakenduse päringule kaasa ülemääraseid andmeid (nt sisestada veebisaidi vormile/lahtrisse suur arv märke).	
Aruandlus	Kooskõlas ISACA IS auditeerimise standarditega tuleb koostada aruanne, mis sisaldab muuhulgas järgmist: • Käsitlusala määratlus • Eesmärgid • Tehtud töö kestus • Sooritatud läbistustestimise ja nõrkuste analüüsi olemus, ajastamine ja ulatus. • Järeldus meetmete toimivuse ja avastatud nõrkuste tähtsuse kohta.	
	Teha uus läbivaatus, millega saada mõistlik kinnitus, et meetmed on teostatud ning kõikide teadaolevate nõrkuste turvaaugud on suletud.	
	Sooridada täpne perimeetri tulemüüride ja ruuterite protsesside ja atribuutide läbivaatus ning arutada tuvastatud riske juhtkonnaga.	

11. JÕUSTUMISKUUPÄEV

11.1 See protseduur kehtib kõikidele IS audititele, mis algavad või toimuvad pärast 1. septembrit 2004. Täielik sõnaseletuste kogu asub ISACA veebilehel *www.isaca.org/glossary*

Protseduur P8. Turbe hindamine – läbistustestimine ja nõrkuste analüüs (jätkub)

LISAD

Toetumine COBITile

Järgnev valik kõige asjakohasematest materjalidest COBITis, mida saab rakendada konkreetse auditi ulatuses, põhineb spetsiifiliste COBITi IT-protsesside valikul ja COBITi teabekriteeriumite arvessevõtmisel.

See protseduur toetub järgmistele COBITi protsessidele:

- PO6 – Teavitada juhtimissihid ja suund
- PO9 – Kaalutleda riskid
- HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
- TT5 – Tagada süsteemide turvalisus
- TT7 – Koolitada kasutajaid
- TT10 – Hallata probleeme

Kõige asjassepuutuvamad kriteeriumid on:

- esmajärjekorras: konfidentsiaalsus, terviklus ja käideldavus;
- teises järjekorras: toimivus ja usaldatavus.

Allikad

Bosworth, Seymour; Michel E. Kabay, Editor; Computer Security Handbook, 4th edition, John Wiley & Sons, Indianapolis, Indiana, USA, April 2002

The CERT Guide to System and Network Security Practices, 1st Edition, Addison-Wesley Publishing Co., June 2001

e-Commerce Security: Security the Network Perimeter, IT Governance Institute, Rolling Meadows, Illinois, USA, 2002

Klevinsky, T.J.; Scott Laliberte; Ajay Gupta; Hack I.T.—Security Through Penetration Testing, Addison-Wesley, Boston, Massachusetts, USA, June 2002

Kreutz, Vines,;"The CISSP Prep Guide;" John Wiley & Sons, Inc.; 2001

Rhoades, David; "Hacking and Securing Web-based Applications," Maven Security Consulting Inc., 12th USENIX Security Symposium, Washington, DC, USA, 4-8 August 2003

Scambray, Joel; Stuart McClure; George Kurtz; Hacking Exposed—Network Security Secrets & Solutions, 2nd Edition, Osborne/McGraw-Hill, Berkeley, California, USA, 2001

Yeager, Nancy J.; Robert E. McGrath; Web Server Technology, Morgan Kaufmann Publishers Inc.

Protseduur P9. Krüpteerimismetoodikate halduse meetmete hindamine

1 SISSEJUHATUS

1.1 Toetumine COBITile

1.1.1 Käesolevates juhistes käsitletava ala läbivaatamisel toetuda spetsiifiliste eesmärkide või protsesside puhul COBITi omadele. Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ja arvestades COBITi teabekriteeriume.

1.1.2 Auditi sooritamisel tuleks lugeda asjassepuutuvaiks COBITi juhised järgmiste protsesside kohta:

- PO8 "Tagada vastavus välisnõuetele",
- TT5 "Tagada süsteemide turvalisus",
- TT11 "Hallata andmeid".

1.1.3 Krüpteerimistehnoloogia auditi seisukohalt kõige asjakohasemad teabekriteeriumid on

- eelkõige: toimivus, konfidentsiaalsus, terviklus, käideldavus ja vastavus;
- teises järjekorras: tõhusus ja usaldatavus.

1.2 Krüpteerimise alused

1.2.1 Krüpteerimine on vahend, millega muundada loetaval kujul olevad andmed (neid nimetatakse avatekstiks) loetamatule kujule (mida nimetatakse krüptogrammiks). See määratlus eristab krüpteerimist kodeerimisest, mille puhul avatekst asendatakse ühe või mitme märgiga (näiteks: "üks, kui rongiga, kaks, kui laevaga").

1.2.2. Andmeid krüpteerivat matemaatilist algoritmi nimetatakse šifriks. Enamik nüüdisaegseid šifreid krüpteerib avateksti mingi võtmega, st teatava salajase teabelõiguga, mida teavad ainult selleks volitatud pooled. 17. sajandiks jõudsid krüptograafid arusaamisele, et krüpteeritud andmete salastatuse säilitamine sõltub mitte algoritmi või šifri sisemiste protsesside, vaid võtme salajas hoidmisest.

1.2.3 Krüpteerimistehnoloogia annab turvameetme, mis kaitseb loetavat teavet juurdepääsu eest, kuid ei piira juurdepääsu mitteloetavatele andmepakettidele. Krüptograafilisi vahendeid saab kasutada andmetervikluse tagamiseks, kuid avatekstsõnumi krüpteerimine krüptogrammiks ei taga iseenesest mitte midagi muud peale andmete konfidentsiaalsuse.

1.2.4 Käesolev protseduur sisaldab hindamisnõudeid selliste organisatsioonide ja asutuste jaoks, kus ei nõuta tippsalastusega turvalisust. On olemas alternatiivseid andmete krüpteerimise meetodeid, mille puhul on võtmed seadmetesse sisse ehitatud; see tõstab krüpteerimisvõtmete ohjega individuaalsete tööjaamade kasutamise usaldatavust. Käesolev protseduur ei hõlma aga sellega seotud spetsifikatsioone.

Protseduur P9. Krüpteerimismetoodikate halduse meetmete hindamine (jätkub)

1.2.5 Reas maades, sealhulgas USAs, on valitsus kehtestanud kitsendusi krüpteerimist rakendavate toodete ekspordile. Need on mõeldud kitsendama selliste toodete kasutamist, mis võiksid muuta vaenulike riikide side luureasutustele dešifreerimatuiks.

1.3 Krüpteerimise kasutamise riski kaalutlemine

1.3.1 Krüpteerimise väga oluline aspekt on otsustus, milliseid andmeid tuleks krüpteerida ning kus ja millal tuleks seda teha. IS audiitor peaks dokumenteeritud riskikaalutluse või kirjaliku poliitika kaudu saama mõistliku kinnituse sellele, et krüpteerimise rakendamisel hinnatakse järgmisi juhtimisaspekte.

- Krüptograafiasüsteemi väga oluline aspekt on hinnata ja otsustada, millised andmed on tundlikud ja tuleks krüpteerida. Teatavad andmed ei sisalda mingit tuvastatavat või eristatavat teavet ega saa kandideerida krüpteerimiseks, kui selleks ei ole konkreetset ärivajadust. Et saada teada, millised andmed (või andmekogumid) on tundlikud ja kas neid peaks krüpteerima, tuleks sooritada riski kaalutlemine. Peale selle on kriitiliseks varaks peetavate andmete konfidentsiaalsuse kaitsmiseks muid vahendeid. Näiteks allub suur haigla, mis pidevalt annab kindlustusseltsile üksikpatsientide kohta meditsiiniteavet, piisavalt olulisele riskile, mis õigustab otspunktkrüpteerimist võimaldava virtuaalse privaatvõrgu kasutamist. Kokkuvõttes tuleks hinnata kõiki andmeid lubamatu vaatamise ja õigustatud ärivajaduse seisukohalt, arvestades riski vähendamise tulu ja kulu.
- IS audiitor peaks hindama võimalikke andmete transportimiseks kasutatavaid teid ja seda, kes saab juurdepääsu andmetele. IS audiitor peaks arvestama, et praegu üldsusele kättesaadavate vahenditega saab andmeid kergesti transportida väljapoole organisatsiooni ning müüa neid konkurendile või rikkuda privaatsuse kaitse seadusi (näiteks USA tervishoiukindlustuse seadust HIPAA). Niisuguste meetodite hulka kuuluvad vähemalt elektrooniline edastus läbi tulemüüri või andmete kopeerimine CD-le, mis seejärel viiakse organisatsiooni territooriumilt füüsiliselt välja. Peale selle on võimalik kasutada võrgu kaudu transporditavate ja tundlikku teavet (näiteks paroole) sisaldada võivate andmepakettide hankimiseks muid tarkvaravahendeid. Seetõttu peaks IS audiitor rakendatavate krüpteerimismeetodite hindamisel eeldama halvimate juhtude stsenaariume.
- Andmeid võidakse krüpteerida mingis tsentraalses kohas või lasta neil olla avateksti kujul tsentraalses kohas ja krüpteerida siis, kui nad transporditakse lõppkasutajale. Otsustus, millal ja kus neid tuleks krüpteerida, on väga oluline. Andmete turvalisuse määrab kõige nõrgem või puuduv turvameede, mis kaitseb andmeid lubamatu vaatamise eest.

Protseduur P9. Krüpteerimismetoodikate halduse meetmete hindamine (jätkub)

- Näiteks peaks võtmete ning muu krüpteerimise tüüpi ja rakendamist puudutava teabe turve võimaldama seda teavet saada ainult neil, kellel on selleks tööalane vajadus. Kui hetke ärivajadused seda rangelt nõuavad, peaksid turbehaldus töötajad ka paroolid ja võtmed krüpteerima, nii et juurdepääs võtmele oleks ainult neil. Mitte mingit teavet, mis puudutab krüpteerimist, ei tohiks hoida arendus- või testimiskeskkonnas, vaid kogu sellist teavet tuleks hoida tootmiskeskkonnas, kus juurdepääs on rangelt kitsendatud. Teine näide: üht ja sama krüpteerimisvõtit ei tohiks kasutada testimiskeskkonnas ja tootmiskeskkonnas.
- IS audiitor peaks veenduma, et on olemas krüpteerimist puudutav poliitika, mis määrab, millal tuleks krüpteerimist rakendada, millist tüüpi ja millisel kujul andmetele, milline peab olema krüpteerimisvõtmete tugevus, millist meetodit kasutada krüpteerimiseks ja kuidas tuleb võtmeid vahetada.
- Andmed, mis krüpteeritakse mingis tsentraalses kohas ning seejärel võetakse sealt krüpteeritud kujul ja saadetakse kasutaja tööjaamale, kus nad dekrüpteeritakse, võivad olla väga turvalised nii oma lähtekohas kui ka transportimisel. Alternatiivse meetodina võidakse andmeid hoida andmebaasis krüpteerimata kujul ning krüpteerida neid ainult siis, kui neid transporditakse. See meetod osutub vähem turvaliseks, kui korvavate meetmete puudumisel võidakse saada lubamatu juurdepääs, kuid tema kasutamise põhjuseks võib olla kompromiss töötlusvajaduste ja turvalisuse vahel. Konkreetsemalt, kui andmeid andmebaasis või failis pidevalt värskendatakse (tugevalt tehinguline hoidla), võib krüpteerimine tsentraalses hoidlas olla ebasobiv, erinevalt staatilisest hoidlast (kus andmeid ei muudeta). IS audiitor ei tohiks küll teha otsustusi selle kohta, kus ja millal tuleb andmeid krüpteerida, kuid ta peaks uurima, kas juhtkond on parima võimaliku otsuse tegemiseks täielikult hinnanud kõiki tingimusi.

1.3.2 Krüpteerimisprotsessi rakendamise hindamisel tuleb arvestada mitmeid tegureid. Näiteks tuleb andmete krüpteerimise puhul teha üldine otsus ühesuunalise või pööratav räsimise kasutamise kohta. Juhtimisotsuste ühe osana tuleks dokumenteerida järgmised kaalutlused.

- Ühesuunaline räsimine krüpteerib andmed ega võimalda neid enam dekrüpteerida. Süsteemis olevaid krüpteeritud andmeid võrreldakse kliendi sisestatud ja järgnevalt krüpteeritud andmetega. Kui need kaks väärtust on võrdsed, on kasutaja sisestatud andmed autenditud. Ühesuunalist räsimist kasutatakse tavaliselt paroolide krüpteerimiseks, kusjuures süsteemi administraatoril on ainult õigus parooli lähtestada, mitte aga parooli näha. Ühesuunalist räsimist kasutatakse tavaliselt veebivõimeliste rakenduste paroolide krüpteerimiseks; seal võib see meetod olla turvalisem kui pööratav räsimine. Üks selle meetodiga seotud riske on võimatus taastada suurt arvu klientide paroole kliendiandmebaasi hävimise korral. Niisugusel juhul tuleb organisatsioonil võib-olla lasta kõigil töötajatel oma isiklikud volitused taas valideerida ja saada uus parool, see aga võib kahjustada organisatsiooni mainet.

- Pööratav räsimine võimaldab andmeid krüpteerida ja dekrüpteerida. Suurem selle meetodiga seotud risk on selles, et võidakse võtta ebasobiv krüpteerimisvõti ja kõiki tundlikke andmeid, sealhulgas paroole, saab paljastada. Seevastu saab andmebaasi rikkumise korral kiiresti taastada krüpteeritud andmed, vältides maineprobleeme. Vajalikud on täiendavad korvavad turvameetmed, millega tagada, et krüpteerimisvõti oleks tugevam, täielikult kaitstud sisemise juurdepääsu eest ja et teda vahetataks sagedamini.

1.3.3 IS audiitor peaks saama mõistliku kinnituse sellele, et enne rakendamist pööratakse võimalikult suurt tähelepanu mitmesugustele andmete konfidentsiaalsust ähvardavatele halduslikku tüüpi riskidele. Teiste sõnadega, kõik krüpteerimise nõrkused ei ole loomult tehnilised ning IS audiitor peaks selgelt hindama juhtkonna otsustusprotsessi veendumaks, et langetatakse kõige toimivam otsus.

1.3.4 Andmete transportimiseks krüpteeritud kujul on palju kolmandate poolte tooteid. Valimisprotsess peaks arvestama vajadust kasutada neid mitmel arvutiplatvormil (Unix, Windows), nii et oleks tagatud kasutamise ühtlus. Peale selle on vahendeid, mis automaatselt soodustavad krüpteerimist, näiteks Unixi turvaline kest (ssh).

1.3.5 IS audiitor peaks mõistma andmeid ümbritsevate turvameetmete, sealhulgas andmete pääsupunktide hindamise tähtsust. Ja lõpuks, kõigile õigusnormidele vastavuse tagamiseks tuleks sooritada vastutuse ja krüpteerimismeetodite õiguslik läbivaatus.

1.4 Kolm nüüdisaegsete šifrite põhikuju

1.4.1 Sümmeetriliste võtmetega krüptograafia (seda nimetatakse ka salajase võtmega krüptograafiaks) kasutab sõnumi krüpteerimiseks ja dekrüpteerimiseks üht ja sama võtit. Sümmeetriliste võtmetega šifrid on kiiremad kui asümmeetriliste võtmetega šifrid, kuid krüptograafe on sajandeid vaevanud vajadus edastada võtmeid, hoides need volitamatute eest salajas. Sümmeetriliste võtmetega nüüdisaegsed šifrid on näiteks DES, Blowfish, Twofish, CAST, IDEA, 3DES ja AES.

1.4.2 Avaliku võtmega krüptograafia (asümmeetriliste võtmetega krüptograafia) kasutab võtmepaari ning ühe võtmega krüpteeritud sõnumit saab dekrüpteerida ainult teise sellesse paari kuuluva võtmega.[5] Avaliku võtmega süsteemi kasutajad avalikustavad ühe võtme, teise aga hoiavad salajas. Kui saatja soovib vastuvõtjale saata krüpteeritud sõnumi, võtab ta vastuvõtja avaliku võtme ja krüpteerib sellega avateksti. Kui vastuvõtja saab enda avaliku võtmega krüpteeritud sõnumi, on ainult temal võti, millega dekrüpteerida sõnumit. Näiteid: Diffie-Hellmani algoritm (DH) ja Rivesti-Shamiri-Adelmani algoritm (RSA). Peale selle loetakse kirjutaja privaatvõtmega krüpteeritud sõnum privaatvõtme omaniku poolt signeerituks.

[5] See ja kogu alajaotis 1.4.2 üldse on üsna ebatäpne ja eksitav, eriti viimane lause. Tegelikult on nii saatjal (S) kui ka vastuvõtjal (V) kummalgi oma võtmepaar, mis koosneb avalikust võtmest ja privaatvõtmest. S krüpteerib avateksti V avaliku võtmega, dekrüpteerida seda krüptogrammi võimaldab ainult V privaatvõti. Signeerimiseks kasutab S oma privaatvõtit, signatuuri kontrollida saab aga S avaliku võtmega igaüks. Tõlkija m.

Kirjutaja avalikku võtit kasutades saab sõnumit dešifreerida ja lugeda igaüks, aga sõnumit luua või muuta saab ainult privaatvõtme omanik, seega on tagatud sõnumi terviklus ja autentsus.

1.4.3 Ühesuunaline räsimine (ühesuunaline krüptograafia, sõnumiautentimiskoodid (MAC), sõnumilühendid) krüpteerib andmed pöördumatule kujule. Ühesuunaline räsimine kasutab avateksti mitte eraldi teabeüksusena, vaid võtmena ja tekitab selle avateksti püsipikkusega lühendi või räsi. Räsifunktsioone tuntakse ühesuunaliste funktsioonidena ning räsist ei ole võimalik tuletada avateksti. Ühesuunalist räsimist kasutatakse tihti andmetervikluse tagamiseks ja paroolide salvestamiseks arvutisse krüpteeritult. Algoritmide näiteid: MD5 ja SHA-1.

1.5 Tavalised krüpteerimise rakendused

1.5.1 Krüptograafiat saab kasutada järgmiste turvaaspektide tagamiseks.

- Konfidentsiaalsus. Tagatakse, et andmeid saavad vaadata ainult ettemääratud pooled. Edastatavate andmete konfidentsiaalsuse tagamise peamine vahend on sümmeetriliste algoritmide kasutamine, kuid väiksemate andmemahtude puhul kasutatakse ka asümmeetrilist (avaliku võtmega) krüptograafiat.
- Andmeterviklus. Tagatakse, et andmed ei ole muutunud, et vastu võetakse samad andmed, mis saadeti. Andmetervikluse saab tagada digitaalsignatuuride (digitaalallkirjade) ja räsimisalgoritmidega.
- Kasutaja autentimine. Vahend, millega tõendatakse, et kasutaja, server või muu olem on see, kes ta väidab end olevat. Autentimiseks saab kasutada asümmeetrilist krüptograafiat, salajase võtme teadmise kontrollimise teel.
- Salgamise vääramine. Tagatakse, et tehing või sõnum tuli isikult, kellelt ta pidi tulema ja ei ole muutunud. Elektrooniliste maksete ja kaubanduse dokumentatsiooni puhul on salgamise vääramine keskne nõue. Saatja ei saa hiljem eitada, et sõnumi saatis tema. See tõendus peab olema piisavalt tugev, nii et seda saaks kasutada kohtumenetluses. Salgamise vääramise võib lühikeste sõnumite puhul saavutada digitaalsignatuuriga või harilikult MAC ja digitaalsignatuuri kombinatsiooniga.

1.5.2 Üks vahend võrguliikluse, eeskätt Interneti kaudu kulgeva HTTP-liikluse (veebiliikluse) krüpteerimiseks on SSL/TLS ("turvaline soklikiht"/"transpordikihi turve"). Protokolli SSL töötas välja Netscape Communications Inc. ja ta muutus valdkonna faktiliseks standardiks. Selle standardi vaatas läbi Interneti Tehniline Operatiivkogu (IETF), kes andis talle nimeks TLS. Praegu kasutatakse neid kaht nimetust sünonüümidena. SSL kasutab konfidentsiaalsuse, andmetervikluse ja veebiserveri autentimise tagamiseks avaliku võtmega krüptograafia, salajase võtmega krüptograafia ja ühesuunalise räsimise kombinatsiooni. Võimalik on ka kasutaja ja veebiserveri vastastikune autentimine. Interneti kaudu kulgevas suhtluses kasutatakse protokolli SSL tavaliselt seotult avaliku võtme infrastruktuuriga (PKI).

Protseduur P9. Krüpteerimismetoodikate halduse meetmete hindamine (jätkub)

1.5.3 Avaliku võtme infrastruktuur (PKI) on süsteem avalike võtmete jaotamiseks digitaalsertifikaatidega. PKI koosneb poliitikatest, protseduuridest, riistvarast, tarkvarast ja personalist, mis on vajalikud avalike võtmete sertifikaatide loomiseks, halduseks, talletuseks, jaotamiseks ja tühistamiseks. PKI süsteem kinnitab, et sertifikaadiga levitatav avalik võti kuulub teatavale isikule või organisatsioonile. Olemus on selles, et avalikku võtit sisaldava sertifikaadi väljastab kasutajale mingi sertifitseerimiskeskus (CA), näiteks Verisign või Thawte. CA signeerib sertifikaadi digitaalselt, valideerides sellega sertifikaadi ning nii kuulub avalik võti ta väidetavale omanikule. Sertifitseerimiskeskused müüvad digitaalsertifikaate mitmesuguse hinnaga, mis sõltub sertifikaadi tüübist. Sõltuvalt sertifikaadi tüübist tuleb isikul või organisatsioonil võib-olla esitada mingi autentimisvorm, näiteks aadress või krediidiaruanne.

1.5.4 Digitaalsertifikaadid on sertifitseerimiskeskuste esmane väljastusmehhanism avalike võtmete jaotamiseks. Digitaalsertifikaadid sisaldavad andmeid võtme omaniku kohta ja võtme kehtivuse kohta ning avaliku võtme koopiat. Sertifitseerimiskeskus signeerib digitaalsertifikaadid.

1.5.5 Digitaalsignatuurid on sõnumi saatja autentimise vahend. Nad tagavad ka sõnumi tervikluse ja salgamise vääramise. Saatja võtab kokkulepitud andmekogumi ja krüpteerib selle oma privaatvõtmega. Kui vastuvõtja saab need andmed dekrüpteerida saatja avaliku võtmega, said need andmed olla krüpteeritud ainult saatja privaatvõtmega.

1.5.6 "Krüpteerimistehnoloogiad on pääsu reguleerimise lahendused. PKI-põhised lahendused on populaarsed kasutajate autentimise tagamisel ja äritehingute kaitsmisel. PKI tähistab avaliku võtme infrastruktuuri ning tähendab digitaalsignatuuride, sertifitseerimiskeskuste ja nendega seotud riist- ja tarkvara kasutamist lubatava ja kinnitatud äriteabe organisatsioonisisese või organisatsioonidevahelise vahetuse korraldamiseks ja halduseks. [6]

1.5.7 Käesolev protseduur ei püüa uurida mitmesuguseid lähenemisviise krüpteerimistehnoloogiate kasutamisele eri maades ega esitada arvamust süsteemide või tarnijate kohta. Meelespealoetelud püüavad anda IS audiitorile ühe raamstruktuuri, mida kasutada krüpteerimismeetodite õige kasutamise kontrollimist sisaldava auditi sooritamisel. Ta ei ole keskendatud mingile spetsiifilisele keskkonnale, näiteks e-kaubandusele.

1.5.8 Mõnedel juhtudel on võimalik vältida krüpteerimise vajadust, kasutades allika autentimiseks mitmesuguseid meetodeid, näiteks tagasihelistuse protseduuri, kuid sageli on alternatiivid kulukad ja kohmakad. Sageli on krüpteerimistehnoloogiad kuluefektiivsed. Auditid ja läbivaatused peavad keskenduma ka protsessidele, mida juhtkond järgib krüpteerimisele kuuluvate andmete väljaselgitamiseks ja nende isikute väljaselgitamiseks, kellele antakse õigus juurdepääsuks nendele andmetele. Mõistliku kinnituse andmiseks sellele, et andmed on kaitstud tasemel, mida nõuab juhtkond, peaks krüpteerimissüsteemide hindamine hõlmama teadaolevaid nõrkusi.

[6] TechWeb Encyclopaedia.

Protseduur P9. Krüpteerimismetoodikate halduse meetmete hindamine (jätkub)

1.5.9 Tänapäeval on krüpteerimine sisse ehitatud paljudesse turvatoodetesse. Seda võib leida paljudest rakendustest, näiteks turustatakse populaarset DESi taolist 128-bitise võtmega algoritmi, mida kasutatakse elektronposti krüpteerimiseks. Turvalise veebilehe külastamiseks pakutakse tavaliselt protokolli SSL ("turvaline soklikiht"), millega saadav krüpteerimise tugevus sõltub brauseri versioonist. [7]

2 KRÜPTEERIMIST REGULEERIVAD ÕIGUSAKTID

2.1 E-kaubandus

2.1.1 Elektronkaubanduse areng on jäigalt seotud krüptograafia kasutamisega usaldusväärse meetodina korra ja turvalisuse toomiseks Interneti muidu loomulikku anarhiasse.

2.2 Riikide krüptograafiakäsitlused

2.2.1 Enamiku riikide agarus suunata krüpteerimistehnoloogiate arengut oma maa turvalisuse huvides kitsendab väga tugevate krüpteerimistoodete avaldamist ja eksporti. Enamasti valivad riigid krüptograafia käsitlemiseks ühe lähenemisviisi kahest.

2.2.2 Euroopa Liit püüab saavutada side- ja infoteenuste, sealhulgas kodeerimisvahendite ja krüpteerimismeetodite kasutamise ja müügi suuremat liberaliseerimist. EL sunnib liikmesmaid ühtlustama oma kohalikke seadusi EL direktiividega. Euroopa maad näivad olevat väga tundlikud vaba turu ja privaatsuse vajaduste suhtes; seda tõendavad alljärgnevad näited.

- Prantsusmaa tõstis vabalt kasutatava krüptoloogia võtmepikkuse 40-lt bitilt 128-le bitile ning taotleb täielikku vabadust krüptoloogia kasutamisel.
- Soome andis välja rea suuniseid, mis väljendavad ta riiklikku krüptograafiapoliitikat. Need suunised ütlevad, et toetatakse vaba kauplemist krüpteerimistoodetega ning et tugeva krüpteerimise kasutamist ei tohiks kitsendada seaduste ega rahvusvaheliste lepetega.
- Iirimaa kuulutas välja oma tulevase krüptograafiat puudutava seadusandluse kesksed põhimõtted. Kasutajail on õigus saada juurdepääs tugevatele ja turvalistele krüpteerimistoodetele ja valida neid oma privaatsuse kaitsmiseks elektronkaubanduses. Krüpteerimistehnoloogiate valmistus, import ja kasutamine ei allu Iirimaal mingitele reguleerimismeetmetele peale kohustuste, mis on seotud seadusliku juurdepääsuga. Krüptograafiliste toodete eksporti hakatakse reguleerima vastavalt asjassepuutuvatele EL eeskirjadele, mis käsitlevad kaheotstarbeliste kaupade ja tehnoloogiate ning tavarelvade ekspordi reguleerimist.

[7] 2 Ouellette, Tim. Encryption Quick Study. Computerworld. 25 January 1999.

- Hispaania kehtestas sideseaduse, mis tagab vabaduse kasutada sideotstarbeks krüpteerimistarkvara.

2.2.3 Teised riigid, näiteks USA, Kanada ja Vene Föderatsioon, pööravad aga nii sise- kui ka välispoliitikas rohkem tähelepanu maa turvalisusele.

- USA kehtestas e-privaatsuse seaduse ("krüpteerimine kaitseb küberruumis inimeste õigusi rikkumise ja väärkasutuse eest"), kuid seda pole rakendatud. See seadus püüdis tagada vabadust kasutada krüpteerimist seadusliku sidesuhtluse turvalisuse, konfidentsiaalsuse ja privaatsuse kaitsmiseks ning edendada privaatsust ja põhiseaduslikke õigusi digitaalses keskkonnas. Aastal 2000 kehtestas USA valitsus uued krüpteerimisalase ekspordi eeskirjad, mis tunduvalt hõlbustasid USA firmadel ja üksikisikutel laialdaselt eksportida tugevat krüpteerimist levinud toodetes, sõltumata selle tugevusest või kasutatavast tehnoloogiast. HIPAA annab USAs õiguse kasutada krüpteerimist kaitstava tervishoiuteabe edastamisel.
- Tehnoloogia tarnijate, lõppkasutajate ja avaliku arvamuse surve võib suurendada kõigi riikide liberaalsust krüptoloogia kasutamise suhtes.

3 KRÜPTEERIMISTEHNOLOOGIATE PROTSEDUUR

3.1 Suhtluskeskkond

3.1.1 Krüpteerimistehnoloogiat tuleb mingis suhtluskeskkonnas kasutada siis, kui kehtib vähemalt üks järgmistest tingimustest:

- andmeid ei tohi meelevaldselt lisada;
- läbi võrgu kulgev teave on konfidentsiaalne ja teda tuleb kaitsta;
- taotletav teenus tuleb tagada ainult lubatud kasutajatele;
- kasutaja ei pea saama eitada teatava sõnumi saamist (adressaadi autentimine);
- iga adressaat peab olema kindel allika identiteedis (saatja autentimine);
- krüpteerimist nõuab õigusakt või seda peetakse ala parimaks tavaks.

3.1.2 Spetsiifilisi küsimusi hõlmab järgnev meelespea.

Protseduur P9. Krüpteerimismetoodikate halduse meetmete hindamine (jätkub)

Krüpteerimise aspektid	Soovitatavad protseduurid krüpteerimismetoodikate halduse meetmete hindamiseks	√
Organisatsiooni haldus	Kontrollida, kas on olemas kirjalikud protseduurid või poliitikad, mis sisaldavad rollide ja kohustuste selget määratlemist võtmehalduse reguleerimismeetmete alal ning hõlmavad võtmete genereerimist või loomist, laadimist, tootmiskeskkonnale laiendamise reguleeritud protsessi muudatuste puhuks, transportimist, säilitust taastamist, kõrvaldamist ja hävitamist, vargust ning nõutava kasutamise sagedust. Need protseduurid peaksid sisaldama nõudeid võtme turbele ja võtme tootmiskeskkonda üleviimise reguleerimisele.	
	Kontrollida, kas on olemas selgelt määratletud kirjalik protseduur, mis määratleb, milliseid andmeid loetakse tundlikeks ja krüpteerimist vajavaiks. Peale selle kontrollida, kas see protseduur sisaldab nõudeid selle kohta, millal ja kuidas tuleb krüpteerimist rakendada. Konkreetsemalt, teha kindlaks, kas krüpteerimist tuleks rakendada andmetele, mis asuvad staatilises andmebaasis või failis, või ainult siis, kui neid edastatakse Interneti kaudu. Seoses ülalöelduga kontrollida, kas on koostatud ja kinnitatud kaitsmisele kuuluvate andmete ja nende tunnusomaduste loetelu. Seejärel selgitada välja, kas on hinnatud iga kaitstava andmeüksuse rahalist väärtust ja kui suured on kaitsmise kulud. Märkus. Krüpteerimisega antavat täielikku konfidentsiaalsust nõudvate infovarade loetelu läbivaatamisel arvestada järgnevat. Kaitsmata võrgu (Interneti) kaudu edastatavad andmed nõuavad tugevamat turvet kui reguleeritav andmebaas, mis asub sisemise võrgu lõigus, mis toetub ainult spetsiifilistele staatilistele sisemiste tööjaamade IP-aadressidele. Peale selle kontrollida, kas ei toimu topeltkrüpteerimist (nii et andmed on krüpteeritult andmebaasis ja seejärel krüpteeritakse neid edastamisel teist korda), kui sellist lisavajadust ei põhjenda mingi riskikaalutlus. Kokkuvõttes peaks IS audiitor kontrollima, kas on olemas poliitikad ja protseduurid, mille järgi määrata, milline teave tuleb krüpteerida, milline peab olema krüpteerimise tugevus ja milliste meetoditega otsustada, kellel peab olema juurdepääs selle teabe dekrüpteerimisele. IS audiitor peaks auditeeritavale teatavaks tegema, et krüpteerimistehnoloogiate edukus põhineb toimival töökorraldusel, mis on sobivalt formaliseeritud.	

Protseduur P9. Krüpteerimismetoodikate halduse meetmete hindamine (jätkub)

	Kontrollida, kas juhtkond on kehtestanud turvameetmed, millega hõlmatakse mingi hulk krüptograafilise süsteemi haldusega seotud käsiprotseduure ja inimesi, ning kontrollida vähemalt järgmisi tingimusi. Kõik füüsilist käsitlust vajavad võtmed peaksid olema kaksikkontrolli all. Krüptograafiliste süsteemide tugevus sõltub võtmete salastatusest. Ideaaljuhul ei tohiks kellelgi olla võimalik käidelda krüpteerimisvõtmeid ega neid näha. Võtmed peaksid koosnema kahest eraldi võtmekomponendist ja nad peaksid olema teada ainult jaosteadmuse ja kaksikkontrolli tingimustes. Võtmeid tuleb hoida arvutis, millele ei ole juurdepääsu programmeerijatel ega kasutajatel; näiteks marsruuteril, mille loogilist juurdepääsu reguleeritakse, millel on tugevad füüsilised turvameetmed ning mida hoitakse mingis turvalises eraldatud alas või ruumis.	
Krüptograafilise süsteemi kavandamise kriteeriumid	Kontrollida, kas protsess, mida ettevõte kasutab krüpteerimisalgoritmi valimiseks, on kõige toimivam ja tõhusam. Kui juhtkond otsustab, millist algoritmi valida parimana, tuleks tal võtta arvesse keskkond, milles krüptograafiline süsteem peab töötama: rahuldavat integratsiooni tagav töötluse tüüp ja edastussüsteem; edastusteed, sealhulgas tihendusnõuded teenusetasemete tagamiseks; kasutajate ja operaatorite oskused ja koolitus süsteemi ja võtme kasutamise alal; turvalist ja usaldatavat suhtlust tagav integratsioon töökeskkonnaga; algoritmi toimivus rakenduse ja eesmärkide seisukohalt.	
	Hankida juhtkonnalt ja vaadata läbi dokumentatsioon, mis tõendab, et valitud algoritm tagab kõikjal (vastavalt riskianalüüsile) soovitud tugevusega kaitse ning on kuluefektiivne ja mugav. Tugevam krüpteerimissüsteem võib näiteks olla kallis ja tarbida suuri arvutiressursse, kuid mitte olla vajalik, arvestades organisatsioonisisesteks edastusteks vajatavat kaitset.	
	Kontrollida, kas juhtkond on teinud koostööd teiste IT-talitustega, tagamaks minimaalset mõju liidestusele ja teistele süsteemidele. Sellise krüptograafilise süsteemi valimisel tuleks arvestada kõiki olulisi tegevusliine, näiteks süsteemiprogrammeerimist ja Unixi administreerimist IT-talituses, samuti andmete konfidentsiaalsuse ja tervikluse vajadusi, võttes arvesse kaitsmisele kuuluvate andmete tähtsust (ja majanduslikku väärtust). Kontrollida integratsiooni süsteemiarhitektuuriga. Krüpteerimissüsteem ei tohiks häirida normaalset tööd ega mõjutada süsteemiarhitektuuri.	
	Hankida juhtkonnalt dokumentatsioon, mis tõendab, et valitud algoritm hoiab volitatud kasutajate dešifreerimiskulud piisavalt madalal tasemel. Sedamööda, kuidas arvutid muutuvad kiirematteks, on vaja uusi algoritme ja pikemaid võtmeid. Krüpteeritud sõnumi dešifreerimise kulud ei tohiks ületada kaitstava teabe enda väärtust.	
	Teha kindlaks, kas juhtkond on rakendanud tunnustatud standardeid krüptograafilise süsteemi ühildamiseks rakendustega. Krüpteerimissüsteemide (näiteks SSL) tarbeks on olemas standardid, mis tagavad ühilduvuse mitmesuguste riistvara- või tarkvaraplatvormide vahel.	
	Kontrollida, kas juhtkond on (seal, kus vaja) arvestanud ja järginud kõiki kohalikke ja rahvusvahelisi õigusakte. Paljud maad on kehtestanud õigusakte krüpteerimistehnoloogiate kasutamise distsiplineerimiseks. Paljudel tarnijatel on ka tegutsemise eeskirjad.	
	Hankida juhtkonnalt ja vaadata läbi dokumentatsioon, mis tõendab, et süsteem on tugev ja ründekindel. Kui sõnumi kinnipüüdja teab krüpteerimisalgoritme või kasutatavat riistvara või tarkvara, ei kahjusta see usaldatavust. Võtme genereerimiseks on võib-olla otstarbekam kasutada tuntud ja testitud algoritmi, mitte aga luua organisatsioonile oma algoritmi. Heade (tugevate) krüpteerimissüsteemide turvalisus sõltub mitte algoritmi salastusest, vaid võtmete salastusest.	

Protseduur P9. Krüpteerimismetoodikate halduse meetmete hindamine (jätkub)

Krüptograafilise süsteemi ja võtmehalduse muutuste ohje	Kontrollida auditeerimistestimisega, kas krüptograafilise süsteemi muudatusi ja ajakohastusi ohjavad ja sooritavad ainult selleks volitatud isikud vastavalt olemasolevatele kirjalikele poliitikatele ja protseduuridele. Kontrollida, kas võtme edastust ohjatakse vastavalt mingile spetsiifilisele protseduurile. Kui võtit on vaja edastada vastuvõtja(te)le, on võtme paljastamise risk suurem. Teha kindlaks, kas võtmete ajapõhine kõrvaldamine vastab poliitikale või ala parimatele standarditele. Väärad või asjatud vahetamised ja ajakohastused võivad kahjustada krüptograafilise süsteemi toimivust. Võtmete sisestamisega rakendustesse tuleks olla ettevaatlik, sest see kujutab endast turvanõrkust. Konkreetsemalt, võtmeid tuleks säilitada ainult sekkumiskindlates moodulites, mitte kunagi aga programmide või operatsioonisüsteemide avatekstis, kus võtmed võidakse paljastada juhtkonna teadmata. Võtmeid peaks tootmissüsteemi üle viima ainult valitud turvapersonal ning seda tuleks teha ainult sellistel perioodidel, mil säilitatakse üleviimise turvalisus. Võtmete koopiaid ei tohiks hoida testimiskeskkonnas ega mingis sellises keskkonnas, kus neile on juurdepääs programmeerijatel ja kasutajatel. Veenduda, et kasutajad ja operaatorid ei käitle võtmeid. Krüpteerimisvõtmete paljastamise riski võivad vähendada automaatsed võtmehalduse süsteemid.	
	Kontrollida, kas krüptograafilise süsteemi võti tagab kõik nõutavad omadused, sealhulgas võtme pikkuse, koostise ja halduse osas.	
	Kontrollida, kas krüptograafilise süsteemi võtit on kerge genereerida ja muuta, nii et võtit saaks kiiresti vahetada paljastamise kahtluse korral ja perioodiliselt vahetada vastavalt nõuetele.	
	Veenduda, et krüptosüsteemile juurdepääsu andva võtme halduslik rakendamine (või parool ta kasutamiseks) ei ole kergesti äraarvatav.	
	Turvainseneri või asjakohase auditeeritavaga arutades veenduda, et krüptograafilise süsteemi või algoritmi kasutamise hõlpsust arvestades on krüptograafilise süsteemi võtit kerge muuta. Andmete lubamatu vaatamise riski tõttu võib olla nõutav võtme sagedane vahetamine.	
Digitaal-signatuur	Teha kindlaks, kas juhtkond on kehtestanud meetmed privaatvõtmete varukopeerimise vältimiseks. Privaatvõtme varukopeerimine suurendab paljastamise riski. Varukoopiad tuleks aga teha avalikest võtmetest, nii et oleks võimalik verifitseerida vanu signatuure pärast nende aegumist või tühistamist.	
	Teha kindlaks, kas juhtkond kasutab krüpteerimiseks ja digitaalsertifikaatideks erinevaid võtmepaare. Riigiasutused võivad nõuda krüpteerimise privaatvõtit. Asjakohastel juhtudel tuleb aga veenduda, et riigiasutus ei saaks koos selle võtmega ka digitaalsignatuuri võtit.	
Krüptograafilise algoritmi kõlblikkuse tingimused	Kontrollida, kas juhtkond on arvestanud vajadust kasutada nii keerulisi matemaatilisi võrrandeid ja valemeid, et oleks välditud nende lahendamine läbisorimislike, analüütiliste ja statistiliste rünnetega. Töökindlus on omadus, mis tagab, et ilma krüpteerimisvõtmeta on võimatu taastada kogu teksti ka siis, kui sissetungijale on teada algoritm, avateksti mingi osa ja sellele osale vastav krüptogramm.	
	Kontrollida, kas juhtkond on matemaatiliselt vähemkeerukate algoritmide kasutamisel võtnud arvesse, et sõnumi taastamiseks vajalikud kulud (programmeerimissammude või arvuti mälu kasutamise kujul) ja aeg peaksid olema peletavad. Dešifreerimise kulud peaksid ületama selle teabe väärtuse, mida krüptosüsteem on mõeldud kaitsma .	

Protseduur P9. Krüpteerimismetoodikate halduse meetmete hindamine (jätkub)

4 JÕUSTUMISKUUPÄEV

4.1 See protseduur kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. jaanuaril 2005 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

LISA

Allikaviide

Fred Piper, Simon Blake Wilson, John Mitchell. Digital Signatures Security & Controls. IT Governance Institute, USA. 1999.

Protseduur P10. Ärirakenduse muutmise ohje

1 TAUST

1.1 Seos standarditega

1.1.1 Standard S6 "Audititöö sooritamine" määrab: "IS auditi personalile tuleks rakendada järelevalve mõistliku kinnituse saamiseks sellele, et auditi eesmärgid saavutatakse ja kohaldatavaid kutsealaseid auditeerimisstandardeid järgitakse. Auditi käigus peaks IS audiitor hankima auditi eesmärkide saavutamiseks piisavad, usaldusväärsed ja asjassepuutuvad asitõendid. Auditi leide ja järeldusi tuleb toetada nende asitõendite analüüsi ja tõlgendamisega.

1.2 Seos COBITiga

1.2.1 Lai juhtimiseesmärk HE2 (hankida ja evitada rakendustarkvara) määrab: "Rakendustarkvara hankimise ja hooldamise IT-protsessi juhtimist, mis rahuldab ärinõuet luua automatiseeritud funktsioone, mis toimivalt toetavad äriprotsessi, võimaldavad funktsionaalsete ja käitusnõuete spetsiifiliste määrangute sõnastamine ja järgustatud, selgete saadustega teostus, kusjuures võetakse arvesse

- funktsionaalne testimine ja vastuvõtmine,
- rakenduste turvameetmed ja -nõuded,
- dokumenteerimisnõuded,
- rakendustarkvara elutsükkel,
- ettevõtte teabe arhitektuur,
- süsteemiarenduse elutsükli metoodika,
- kasutaja ja masina vaheline liides,
- paketi individualiseerimine."

1.2.2 Lai juhtimiseesmärk HE3 (hankida tehnoloogia infrastruktuur ja hooldada seda) määrab: "Tehnoloogia infrastruktuuri hankimise ja hooldamise IT-protsessi juhtimist, mis rahuldab ärirakenduste toetuseks sobivate platvormide loomise ärinõuet, võimaldavad mõistlik riistvara ja tarkvara hankimine, tarkvara standardimine, riistvara ja tarkvara soorituse hindamine ning järjekindel süsteemihaldus, kusjuures võetakse arvesse

- vastavus tehnoloogia infrastruktuuri suundadele ja standarditele,
- tehnoloogia hindamine,
- installeerimis-, hooldus- ja muutmismeetmed,
- ajakohastuse, konversiooni ja migratsiooni plaanid,
- sisemiste ja väliste infrastruktuuride ja/või ressursside kasutamine,
- tarnijate kohustused ja tarnijasuhted,
- muudatuste haldus,

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

- omamise kogukulud,
- süsteemitarkvara turvalisus."

1.2.3 Lai juhtimiseesmärk HE6 (“Hallata muudatusi”) määrab: "Muutuste haldamise IT-protsessi juhtimist, mis rahuldab ärinõuet minimeerida katkestuste, volitamata muudatuste ja vigade tõenäosust, võimaldab haldussüsteem, mis tagab kõigi olemasolevas IT infrastruktuuris taotletavate ja tehtavate muudatuste analüüsi, teostuse ja järelkäsitluse, kusjuures võetakse arvesse

- muudatuste identifitseerimine,
- liigitamine, prioriteetide andmine ja hädaprotseduurid,
- mõjude hindamine,
- muudatuste volitamine,
- väljalaske haldus,
- tarkvara jaotamine,
- automatiseeritud vahendite kasutamine,
- konfiguratsioonihaldus,
- äriprotsessi ümberkavandamine."

1.2.4 Lai juhtimiseesmärk PO9 (kaalutleda riskid) määrab: "Riskide kaalutlemise IT-protsessi juhtimist, mis rahuldab ärinõuet toetada juhtimisotsuseid IT eesmärkide saavutamisega ja ohtudele reageerimisega, vähendades keerukust, suurendades objektiivsust ja piiritledes olulised otsustustegurid, võimaldab organisatsiooni enda tegelemine IT riski tuvastuse ja mõju analüüsimisega, kaasates multidistsiplinaarseid funktsioone ja rakendades ökonoomseid vahendeid riskide leevendamiseks, kusjuures võetakse arvesse

- riskihalduse omanikud ja vastutus,
- IT riskide eri liigid (tehnoloogia-, turva-, jätkusuutlikkus-, regulatsiooni- jt riskid),
- määratletud ja teatavaks tehtud riskitaluvuse profiil,
- juurpõhjuse analüüsid ja riskikäsitluse ajurünnakuseansid,
- kvantitatiivne ja/või kvalitataiivne riski mõõtmine,
- riski kaalutlemise metoodika,
- riskialane tegevusplaan,
- õigeaegne taaskaalutlemine."

1.2.5 Detailne juhtimiseesmärk PO10 (hallata projekte) määrab: "Projektihalduse IT-protsessi juhtimist, mis rahuldab prioriteetide seadmise ning õigeaegse ja eelarve piiresse jääva väljastuse ärinõuet, võimaldab see, et organisatsioon piiritleb ja prioriteedib projektid vastavalt tegevusplaanile ning rakendab igale käsilevõetavale projektile mõistlikke projektihalduse meetodeid, kusjuures võetakse arvesse

- ärijuhtkonna poolne projektide spondeerimine,
- programmihaldus,
- projektihalduse võime,
- kasutajate osalus,
- töö liigendamine, tähtpunktide määratlemine ja järkude kinnitamised,
- kohustuste jaotus,
- range tähtpunktide ja töösaaduste jälgimine,
- kulude ja tööjõu eelarved, sisemiste ja väliste ressursside tasakaalustamine,
- kvaliteedi tagamise plaanid ja meetodid,
- programmi ja projekti riski kaalutlused,
- üleviimine väljatöötusest käitusesse."

1.2.6 [---] [8]

1.2.7 Detailne juhtimiseesmärk TT1 ("Määratleda teenusetasemed ja hallata neid") määrab: "Teenusetasemete määratlemise ja haldamise IT-protsessi juhtimist, mis rahuldab ärinõuet luua ühine arusaam nõutavast teenusetasemest, võimaldab niisuguste teenusetasemelepete sõlmimine, mis formaliseerivad sooritusvõime kriteeriumid, mille järgi hakatakse mõõtma teenuse kvantiteeti ja kvaliteeti; seejuures võetakse arvesse

- formaalsed lepped,
- kohustuste määratlemine,
- reaktsiooniajad ja mahud,
- arveldus,
- tervikluse garantiid,
- konfidentsiaalsuslepped,
- kliendi rahulolu kriteeriumid,
- nõutavate teenusetasemete kulude ja tulude analüüs
- seire ja aruandlus."

1.3 Toetumine COBITile

1.3.1 Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ning arvestades COBITi juhtimiseesmärke ja nendega seotud juhtimistavasid.

[8] Viga lähtedokumendis: siia oli kopeeritud eelmise alajaotise sisu (Tõlkija m.)

1.3.2 Valitavad ja sobitatavad protsessi- ja juhtimiseesmärgid võivad varieeruda sõltuvalt ülesande konkreetsest käsitlusalast ja lähtetingimustest. Selle nõude täitmiseks liigitatakse valitud ja kohandatud COBITi protsessid, mis tõenäoliselt on kõige asjakohasemad, alljärgnevalt.

- Esmajärgulised:
  - PO1 – Määratleda strateegiline IT plaan
  - PO5 – Hallata IT-investeeringuid
  - PO9 – Kaalutleda riskid
  - PO10 – Hallata projekte
  - PO11 – Hallata kvaliteeti
  - HE1 – Tuvastada automatiseeritud lahendused
  - HE3 – Hankida rtakendustarkvara ja hooldada seda
  - HE5 – Installeerida ja akrediteerida süsteemid
  - HE6 – Hallata muudatusi
  - TT1 – Määratleda teenusetasemed ja hallata neid
  - TT3 – Hallata sooritust ja suutvust
  - TT4 – Tagada pidev teenus
  - TT5 – Tagada süsteemide turvalisus
  - TT9 – Hallata konfiguratsiooni
  - TT10 – Hallata probleeme
  - S1 – Seirata protsesse
  - S2 – Hinnata sisejuhtimise adekvaatsust
- Teisejärgulised:
  - PO3 – Määrata tehnoloogiline suund
  - PO6 – Teavitada juhtimissihid ja suund
  - TT7 – Koolitada kasutajaid

1.3.3 Muudatuste ohje puhul on kõige asjakohasemad teabekriteeriumid

- esmajärjekorras: toimivus ja tõhusus;
- seejärel: usaldatavus, käideldavus, vastavus, terviklus ja konfidentsiaalsus.

1.4 Protseduuri eesmärk

1.4.1 See dokument on algselt mõeldud IS sise- ja välisaudiitoritele, kuid seda võivad kasutada ka teised IS spetsialistid, kellel on kohustusi infosüsteemide käideldavuse, andmete tervikluse ja teabe konfidentsiaalsuse alal.

1.4.2 Nüüdisettevõtted on organiseeritud teatava tuumprotsesside kogumina. Peaaegu iga organisatsiooni kogu maailmas ootab ees üha suurem toimivuse ja tõhususe saavutamise surve (st kõrgemad kvaliteedinõuded toodetele ja teenustele, suurema tulu, kulude vähendamise ja uute toodete väljatöötamise vajadus), surve paremate, kiiremate ja odavamate, ettevõtteomanikele kvaliteetsemat tarkvara andvate tarkvara muudatuste ohje protsesside saamiseks.

1.4.3 Kõiki selles protseduuris määratletud testimissamme ei saa rakendada kõigis IT auditites, sest iga üksiku vaatlusaluse arendusprojektiga seotud riskitase on erinev. Mõistliku kinnituse saamiseks sellele, et ohje toimivuse kindlustamine lisab ettevõtte jaoks väärtust, tuleks pidevalt hinnata iga testimissammuga seotud kulusid ja pingutust. Riski kaalutlemise objektiks oleva ülesande eest vastutava auditijuhtkonna otsuse põhjal võivad tavaliselt jääda selles protseduuris nimetatud viisil testimata meetmed selliste riskide leevendamiseks, mida ei loeta kaalukaiks ega olulisteks. Seetõttu on soovitatav sooritada riski kaalutlemine, mille põhjal saaks otsustada, milliseid meetmeid tuleks testida ja milliseid selles protseduuris määratletud auditisamme rakendada.

1.4.4 Selles protseduuris määratletud testimissammude mahukuse tõttu peaks IT auditi juhtkond kaaluma nende viie sammu rakendamist, mida kasutatakse auditi toimivaks plaanimiseks ja sooritamiseks Projektihalduse Instituudi (PMI) projektihalduse metoodikas.

2 SÜSTEEMI ARENGU ELUTSÜKKEL (SDLC)

2.1 Üldeesmärk

2.1.1 SDLC auditi eesmärk on hinnata seda, millises ulatuses vastab hangitud või väljatöötatud süsteem täielikult tarneobjektidele, mis on piiritletud juhtkonna kinnitatud projektitaotluses, hinnata seda, millises ulatuses vastavad hangitud või väljatöötatud süsteemi tegelikud kulud eelarvele, ning teatada tegevjuhtkonnale ja/või juhatuse revisjonikomisjonile, kas projekt vastab piiritletud tarneobjektidele ja on eeldatud kulude piires.

2.1.2 Siseauditi osakonna üldeesmärk SDLC auditi sooritamisel on otsustada, kas

- äriprotsessid ja -süsteemid on kavandatud ja teostatud adekvaatseid sisemeetmeid rakendades;
- projektihaldus on adekvaatne andma mõistlikku kinnitust sellele, et projekti eesmärgid on saavutatud;
- eelarvehinnangud on realiseeritud,
- vajalikud äriotstarbelised funktsioonid on saavutatud,
- projektirühm kasutab süsteemiarendustegevuse, süsteemide kvaliteedi ja organisatsiooni poliitikate järgimise seireks mingit ohjatavat ja struktureeritud metoodikat.

2.1.3 On välja töötatud detailne protsess, millega aidata SDLC rühmal tagada süsteemiarenduse igas järgus

- õigeaegselt tuvastada juhtimisküsimused (süsteemi, äritegevuse, metoodika või projektihalduse alal);
- ettenägelik osalemine sisejuhtimise struktuuri hindamisel projekti kogu elutsükli kestel;
- tulevaste auditite parem katvus äriprotsesside ja -funktsioonide parema tundmise tõttu.

2.2 SDLC järgud

2.2.1 Süsteemi arengu elutsükli iga järgu eesmärkideks kasutatakse spetsiifilisi auditiprogramme. Lisaks sellele kasutatakse üldise projektimetoodika raamstruktuuri auditiprogrammi, mis katab projekti elutsükli kõiki järke. Tüüpiliselt hõlmatakse SDLC auditi peamiste järkudega

- ärinõuete määratlemine,
- projekti algatamine,
- kavandamine ja väljatöötamine (konstrueerimine),
- testimine,
- teostamine,
- teostusjärgsed tegevused.

2.2.2 Kui aga arvestada väljatöötuse mehhanismi, sealhulgas kasutajaliidese kavandamist, tuleb läbivaatuse käsitlusalasse võib-olla võtta täiendavaid juhtimisprotsesse. Seoses selle protsessiga peaks IS audiitor kontrollima kasutajaliidese lahenduse ja rakenduskoodi kooskõla adekvaatsust kogu SDLC protsessis.

2.2.3 Järkude nimed võivad SDLC metoodikates varieeruda, kuid olulised eesmärgid ja tarneobjektid on kooskõlas. Peale selle võivad süsteemiarenduse projekti järgud kulgeda rööbiti ning siirdepunktid pole alati selged. Seetõttu võib mingi järgu tarneobjektide lõpetamine nihkuda järgmistesse järkudesse.

3 KESKSED MEETMETE PUUDUMISE VÕI EIRAMISE RISKID

3.1 Näited

3.1.1 Näited jaotises 3.2 ei hõlma kõike. See teave esitatakse meetmete puudumise riski esiletõstuks.

3.2 Üldine juhtimine ja projektihaldus

3.2.1 Tarkvara muudatuse ja sellele kulutatavate ressursside eest vastutuse kehtestamiseks peaks äritegevuse omanik kinnitama keskse nõutava tarneobjekti dokumentatsiooni (sealhulgas funktsionaalsete nõuete määratluse, tehnilise spetsifikatsiooni, projekteerimis-, väljatöötus-, testimis- ja siirdedokumentatsiooni). Ilma sellise kinnituseta on olemas risk, et IT ja äritegevuse omanikud ei ole sooritatava töö ja lõpptulemi osas ühel nõul.

3.2.2 Tarkvara muudatuse toime hindamiseks peaks projekti- või IT-juht korraldama üksustevahelise nõupidamise teiste IT alade ja äritegevuse omanikega. Need nõupidamised tuleks protokollida ning toimeid tuleks arvestada nõuetes ja lahenduses. Ilma niisuguse toimete hindamiseta võidakse negatiivselt mõjutada teisi allüksusi või vähendada lahenduse toimet.

3.2.3 Tarkvaraarenduse ürituste modulariseerimise (eraldamise) võimaluse tõttu võivad mitmesugused komponendid kavandamise ja väljatöötuse eri harudes kiireneda. See ei tarvitse küll kujutada endast riski, kuid sageli on vaja koostada küsimuste või probleemide loetelusid, milles aga võib-olla ei ole kaudseid probleeme, mis võivad viivitada töö edenemist. Selle loetelu peaksid kinnitama kõik pooled, alates tarkvara väljatöötajaist ning lõpetades äriprotsessi omanikuga ja arendusrühma juhtkonnaga.

4 SDLC METOODIKA

4.1 Ärinõuete määratlemine

4.1.1 Nõuetele, mida peab koostama või täielikult läbi vaatama ja formaalselt kinnitama äritegevuse omanik, on viidatud jaotises 3.2.1. Ilma selle meetmeta võib allüksuste vahel olla lahkarvamusi projektile või taotlusele esitatavate nõuete suhtes ning IT võib jätta loomata sellise funktsionaalsuse, mida vajab see äriüksus.

4.2 Projekti algatamine

4.2.1 Kõik ärirakendustega seotud projektid või taotlused tuleb algatada äriüksuses, sealhulgas ka need, mis puudutavad tarkvara defekte ja täiustusi. Äriüksus peaks määratlema ja/või kokku leppima projekti käsitlusala ja projekti jaoks vajalikud ressursid. Kui seda meedet ei oleks, võiks IT teha uuendusi, muudatusi ja teostada uusi funktsioone äriüksuse teadmata.

4.2.2 Konsultatsioonipunkt otsustab äritegevuse omanikega arutades lahtise küsimuse raskuse ja suunab küsimuse selle põhjal edasi. Kui probleemiavaldustele ei anta sobivaid prioriteete ega suunata õigesti, võidakse ebaotstarbekalt kasutada IT ressursse tarkvara muudatusteks või hoolduseks.

4.2.3 IT peab kasutama kõigi äritegevuse omanikult lähtuvate projektide ja taotluste jälgimiseks mingit jälgimissüsteemi. Konsultatsioonipunkti avaldused ja versiooniohje andmikes peavad olema vastastikused viited. Kui seda meedet ei ole, võidakse projektide algatamine jätta asjakohaselt jäädvustamata ja võib-olla IT juhtkonnale nähtamatuks.

4.2.4 Projekti- või IT-juht peaks otsustama muudatuse mahu ja keerukuse põhjal, milline dokumentatsioon tuleb koostada. Kui seda meedet ei ole, võidakse nõuda liiga vähe või liiga palju (see ei ole kuluefektiivne väikeste projektide puhul, kus kavandamiseks ja väljatöötamiseks kulub alla 30 tunni) dokumentatsiooni meetmete järgimise tõendamiseks.

4.3 Kavandamine ja väljatöötamine (konstrueerimine)

4.3.1 Teha kindlaks, kas funktsioonidesse on pandud korralik juurdepääsu turve, kusjuures äritegevuse omanik on piiritlenud rollid, kellel võib olla juurdepääs uutele funktsioonidele. Kui turve on vajalik, kuid seda pole arvestatud, võib aset leida lubamatu juurdepääs äriteabe vaatlemiseks ja muutmiseks.

4.3.2 Teha kindlaks, kas on olemas versiooniohje. Selle puudumisel suureneb risk viia tootmiskeskkonna koostisse uus moodul või funktsioon IT juhtkonna teadmata ja/või koodi ülekirjutuse risk või alusvariandi halduse puudumise risk.

4.3.3 Teha kindlaks, kas enne teostamist saadakse kirjalik volitus kasutajailt äriüksuses, taotlejalt ja muudelt mõjutatavailt aladelt. Kui seda ei toimu, suureneb risk teostada uus ja/või ebasobiv kood projekti või taotluse kõigi huvipoolte teadmata.

4.4 Testimine

4.4.1 Ärialased kasutajad või nende määratud esindajad väljastpoolt rakenduse väljatöötamise rühma peaksid läbi vaatama testimistingimused ja testimisplaani, veendumaks katvuse õigsuses kogu testimistsüklis. Peale selle tuleks nõuete mahukuse ja keerukuse puhul kasutada viite- või jälitusmaatriksit. Jälitusmaatriks peaks olema kooskõlas testimisjuhtudele, sealhulgas kasutusmallidele esitatavatele nõuetele. [9]

4.4.2 Ärialased kasutajad peaksid läbi vaatama testimistulemused (näiteks kasutaja rahulolu testimise), kontrollides, kas tulemused vastavad nende ootustele. Kui ärialased kasutajad või nende määratud esindajad väljastpoolt IT-rakenduse väljatöötamise rühma ei kontrolli täielikult ega kinnita testimistulemusi, jääb ära testimise tõeline valideerimine ja tõendamine ning selle tulemusena võivad projekti või taotluse nõuded jääda rahuldamata.

[9] Viga lähtedokumendis: osa teksti on puudu (Tõlkija m.)

4.4.3 Rakenduse väljatöötaja IT-juht (või vastav programmeerija järelevalve) peaks tootmissüsteemi viidava(d) koodi (muudatused) läbi vaatama ja kinnitama. Selle meetme puudumisel võib IT juhtkonnal jääda teadmata taotlus lisada tootmissüsteemile uusi funktsioone. Märkus. Sellele meetmele ei tuleks toetuda pettuste avastamiseks.

4.5 Rakendamine

4.5.1 Rakenduse väljatöötajail ei tohiks olla võimalik rakendada koodi tootmiskeskkonnas. Selle meetme puudumise tagajärjeks võivad olla tarkvara volitamatud muudatused. Peale selle võivad ohjamata ja/või volitamata muudatused äriteabes viia pettuse ja korratusteni. Ja lõpuks, tootmiskeskkonda võidakse viia kahjurprogramme, mis mõjutavad süsteemi käideldavuse, andmete tervikluse ja teabe konfidentsiaalsuse aspekte.

4.6 Pärast evitamist

4.6.1 Probleemi- ja konsultatsiooniavalduste käsitlus tuleks lõpetada õigeaegselt ning juurpõhjus ja lahendusmeetod dokumenteerida. Selle meetme puudumisel võivad probleemid korduda, tarkvara muudatuste vajadused võivad jääda tuvastamata ja/või võib jääda mulje, et probleemi käsitlus on veel lõpetamata.

4.6.2 Muude tegevuste hulka võivad kuuluda läbivaatus eesmärkide saavutatuse väljaselgitamiseks ning läbivaatus rakendusele kesksete sisemeetmete ja reeglite rakendatuse väljaselgitamiseks.

5 SDLC-d MÕJUTAV TOOTMISTÖÖTLUS

5.1 Erakorralise muutmise protsess

5.1.1 Standardse muudatuste ohje protsessi erandite käsitluse vahendeid ja meetodeid reguleerivad koos plaanivälise muutmise ja erakorralise muutmise alamprotsessid. Plaanivälise muutmise alamprotsess reguleerib muudatusi, mida põhjustavad tähtaja ületamine ja/või lahknevus sihtide ajakavast. Erakorralise muutmise alamprotsess kehtestab meetmete rakendamise neile vahenditele ja meetoditele, mida kasutatakse kliendi teenusetasemeid otseselt mõjutavate süsteemi tõrgete kõrvaldamiseks. Seega on erakorraline muudatus rakendusprogrammi muudatus, mis tehakse 24 tunni piires, oluliste tõrgete kordumise vältimiseks.

5.1.2 Erakorralise muutmise protsessi tuleks rangelt hallata, nii et standardsest muutmisprotsessist lahknemine kinnitataks eelnevalt. Erakorralise muutmise käigus sooritatavad tegevused logitakse ning need vaatab läbi juhtkond koos rakenduse väljatöötamise ja turvateenuste rühmadega (näiteks seetõttu, et süsteemi käideldavust taastava erakorralise muudatuse tegemiseks antakse programmeerijale suured pääsuõigused). Kui äriline kasutaja on süsteemi taastanud, tuleb sooritada järgmised sammud:

- kõrvaldada programmeerija juurdepääs tootmiskeskkonnale;
- teha täielik järelanalüüs ja leida juurpõhjus;
- teha täielik regressioontestimine, et selgitada välja, kas erakorraline programmi parandus mõjutab süsteemi muid elemente (andmebaasi, rakenduse liidestust, teisi muudetud programmiga samasse komplekti kuuluvaid rakendusi jm);
- kontrollida, kas programmiparandust täidetakse ohjatavast ja varundatud programmiteegist ning kas ta lähtekood säilitatakse muudatuse äri- ja õigusriskil põhineva nõutava aja kestel;
- püsivana mõeldud programmimuudatus viia sisse tarkvara alusvarianti, nii et oleks mõistlikult tagatud muudatuste ülekirjutuse vältimine programmi edaspidiste muutmiste korral.

5.2 Probleemihalduse alamprotsess

5.2.1 Probleemihalduse alamprotsess annab suunatava, süstemaatilise ja ohjatava metoodika niisuguste probleemide lahendamiseks, mis rakenduse muutmise ajal mõjutavad IT-teenuseid. See protsess sisaldab kõiki töid, mis on vajalikud probleemide halduseks elutsükli kestel. Need tööd hõlmavad plaanimise, testimise, rakendamise ja taastamise protseduure teenuse avariijärgsel taastamisel. Selle meetme siht on minimeerida või välistada korduvaid kliendi teenindust mõjutavaid probleeme. Selle protsessi tulem hõlmab tavaliselt erakorralise ja plaanivälise muutmise alamprotsessi. Seda protsessi tuleks uurida üksikasjalikult, sealhulgas seda, kas

- on loodud jälgitavus, kui probleemile on määratud spetsiifiline käsitlus ja igal süsteemil on oma probleemijärjekord;
- erakorralised muudatused kõigepealt dokumenteeritakse täielikult selles alamprotsessis;
- teatavad kliendiga seotud kaebused kõigepealt dokumenteeritakse ja hinnatakse selles protsessis, enne süsteemi muutmise formaalse taotluse esitamist;
- lahendus, sealhulgas probleemi või muudatuse järelanalüüs, on täielikult dokumenteeritud ning sisaldab juurpõhjuse analüüsi ning vahendeid ja meetodeid probleemi õigeaegseks kõrvaldamiseks;
- lahenduse või süsteemi eest vastutav juht on probleemiavalduste käsitluse sulgenud.

5.3 Ühekordsed programmid

5.3.1 Aeg-ajalt luuakse mingi spetsiifilise ja ainulaadse tegevuse vajadusteks programme ühekordseks kasutamiseks. Näiteks võivad vajaduse sellise programmi järele tekitada spetsiifilised andmehalduse teenused. Niisugused programmid tuleb muutmisprotsessis allutada samasugusele programmi riskil ning andmete terviklusel

ja süsteemi käideldavusel põhinevale rangusele, nagu iga muu programmi loomine või muutmine. Nende meetmete edasiseks detailiseerimiseks ja rakendamiseks riski kaalutlemise põhjal vt jaotis 7.3 ("Testimisprogrammis määratletud meetmete rakendamine").

5.4 Tootmiskeskkonna range ohje

5.4.1 Võidi kehtestada tugev muudatuste ohje protsess, kuid IS audiitor peaks kaaluma lisasamme, millega veenduda selle protsessi järgimises (näiteks selles, et programmeerijail pole võimalik sellest protsessist täielikult mööda hiilida). Järgnevas on aspektid, mida IS audiitor peaks arvestama muudatuste ohje protsessi järgimise kontrollimisel, mitte ainult suurtes IS-projektides.

5.5 Avastusmeetmed

5.5.1 Hoolimata kõigist ülalnimetataud meetmetest on programmeerijad piisavalt oskuslikud leidma võimalusi programmide käituseks tootmiskeskkonnas väljaspool muudatuste ohje protsessi või sellest mööda hiilides. Seetõttu on soovitatav, et arvuti käituspersonal või mingi sõltumatu rühm väljaspool rakenduste väljatöötamise rühma seiraks tootmiskeskkonnas toimuvat, et avastada programmeerijate sooritatavaid programmide käitusi (näiteks töid, mille algataja kasutajatunnus kuulub programmeerijale). Selliste avastusmeetmete kehtestamine on soovitatav teabe tervikluse kaitseks.

5.6 Vältimismeetmed

5.6.1 IS audiitor peaks läbi vaatama tootmiskeskkonna andmefailid ja andmebaasid, et teha kindlaks, kas programmeerijail on neile juurdepääs, mis võimaldab uuendamist. Peale selle ei tohiks tootmiskeskkonnas olla kompilaatoreid ega juurdepääsu lähtekoodile ning rakenduste väljatöötajail peaks lähtekoodi kontrollimiseks olema piiratud juurdepääs.

5.6.2 On organisatsioone, kus lugemispääs äriliste ja süsteemiga seotud aruannete genereerimiseks võib olla aktsepteeritav risk, kui tootmisüksus või arvuti käituspersonal sellega eelnevalt nõustub. Tugevad vältimismeetmed väldiksid aga programmide käituse tootmiskeskkonnas väljaspool tööde plaanurit või muud automatiseeritud vahendit, mis reguleeriks programmide täitmist (näiteks ei käivita äriprogramme tavaliselt arvutioperaator käsitsi). Muutmisprotsessi auditeerimise viimane samm peaks olema programmi täitmise konfiguratsiooni loomise läbivaatus tööde plaanuris (näiteks täidetud programmide loetelu läbivaatus), kusjuures tuleks kontrollida, kas kõik tööde plaanuris tehtud muudatused on kinnitanud tootmisüksuse või arvutikäituse juhtkond.

5.7 Halva SDLC-protsessiga seotud riskid

5.7.1 Meetmeid rakendatakse sõltuvalt IT-rühma ja organisatsiooni suurusest ning iga muudatuse mahust ja keerukusest. Seetõttu on vaja luua otsustusmaatriks, mis seob mitmesugused meetmed muudatuste spetsiifiliste tüüpidega (näiteks strateegiliste, suurte, väikeste, taktikaliste või erakorralistega), ja rakendada seda. Kuna see otsustusmaatriks viib meetmete taseme kooskõlla programmimuudatustest tulenevate äririskide aktsepteeritava tasemega, peaks selle maatriksi kinnitama organisatsiooni kõrgem juhtkond.

5.7.2 Protsessi järgimise ja ta uuendusvajaduste uurimiseks on vajalik SDLC perioodiline läbivaatus (IT isehindamine). Kui see meede puudub, kuid arendus- ja evituslahenduste protsesside täiustamiseks uuendatakse SDLC-d pidevalt, võib IT rühm seda mitte järgida või mitte ohjata riske toimivalt ja tõhusalt.

6 ANDMIKUD

6.1 Andmike pidamine

6.1.1 Andmikud peaksid olema piisavalt detailsed, nii et nad võiksid toetada auditi leide ja auditi tulemusena tehtud järeldusi.

6.1.2 Muudatuste ohje protsessi järgimist toetavate auditi asitõendite säilituse aluseks peaksid olema muuhulgas järgmised tegurid:

- teabe maht ja ta arhiveerimisega seotud kulud;
- reguleerivate eeskirjade nõuded;
- muudatuse tähtsus üldiste ärivajaduste seisukohalt;
- vajadus kasutada projekti dokumentatsiooni edaspidisel läbivaatusel SDLC protsessi detailiseerimiseks ja personali soorituse haldamiseks.

7 SDLC ERILÄBIVAATUSED

7.1 Selle protseduuriga hõlmamata läbivaatuste käsitlusala

7.1.1 Käesolevasse protseduuri ei ole lülitatud SDLC eriläbivaatuste nõudeid, mis tulenevad mitmesuguste tarkvara muudatuste ja nendega seotud tehniliste nõuete ainulaadsest iseloomust, sealhulgas spetsiifiliste elementide tuvastamist muutmisprotsessis. Näiteks võib ainulaadseteks lugeda järgmisi tarkvara- ja riistvaraalasid, kuigi neile saab võib-olla rakendada suurt osa järgnevatest meetmetest:

- veebirakenduste SDLC (näiteks skriptründeid ja SQL injektsiooni võimaldavate nõrkuste vältimiseks);
- tarkvara lähtekoodi läbivaatused (näiteks kahjur- või pettusekoodi avastamiseks);
- tehniliste erisüsteemide (EFT-süsteemide) äritarkvara.

7.2 Testimislepe

7.2.1 Muutuste ohje testimise tüübi kohta peaks olema lepe. See leppe aluseks või tõukejõuks peaksid olema üldised tarkvaraprobleemid, näiteks kvaliteedi adekvaatse tagamise puudumine, või äritegevuse katkemised testimise tõttu, samuti muutuste ohje protsessi tasuvus.

7.3 Testimisprogrammis määratletud meetmete rakendamine

7.3.1 IS audiitor peab tingimata tasakaalustama ühelt poolt projekti mahu (vajaliku tööpanuse), nõutava tähtaja ja muudatuse elutähtsuse ning teiselt poolt sobiva meetmete taseme, mis tuleb rakendada protsessile. Seetõttu pole kõik soovitatavad protseduurid rakendatavad kõigile tarkvara muudatustele, eriti kui projekt on väike. Neid meetmeid tuleks aga arutada ja hinnata koos juhtkonnaga, kontrollides riski, mis on seotud nende meetmete puudumisega.

8 MUUDATUSTE OHJE TESTIMISE PROGRAMM

	Soovitatavad muudatuste ohje testimise protseduurid	√
Plaanimine ja haldus	Hindamise iseloomu, ajastuse ja ulatuse põhjal määratleda käsitlusala. Mitmesuguste tarkvara muudatuste kohta tuleks sooritada riski kaalutlemine äritegevuse ja eeskirjade seisukohalt. Valimid tuleks võtta rangelt riski väärtuste alusel, mis hõlmavad ärikeskkonda, eeskirjade nõudeid, kulusid ja tulusid, IT keskkonna toimeid jms.	
	Kõik kesksed meetmed ei kehti kõigi tarkvara muudatuste puhul. Konkreetsemalt, tarkvara muudatuste suurus võib mõjutada kvaliteedi läbivaatuse protsessi tõendamiseks vajaliku dokumentatsiooni rangust. Dokumentatsiooni koostamist nõudvate olukordade piiritlemiseks koostada otsustusmaatriks. Meetmete taset võivad dikteerida organisatsiooni suurus ja muudatuse keerukus. Protsessil tervikuna aga peavad olema adekvaatsed meetmed kohustuste lahutamiseks ja täielikuks testimiseks enne programmi üleviimist tootmiskeskkonda.	
	Teha kindlaks, kas on koostatud dokumentatsioon, mis hõlmab kõiki lahendamata probleeme ja küsimusi SDLC eri järkudes. Kontrollida, kas IS kõrgem juhtkond kinnitab niisuguse lahendamata probleemide (näiteks vaegtööde) loetelu enne järgmisse järku siirdumist.	
	Ülesande memosse lisada lausung selle kohta, et sellele auditile ei saa toetuda kahjurkoodi sisaldava pettuse avastamiseks, sest selleks vajalik tuhandete koodiridade põhjalik läbivaatus võib liigse kulukuse tõttu ära jääda, kui ülesanne ei käsitle spetsiifiliselt seda riski.	
Vajalikud oskused	Tunda IS personali kasutatavat kavandamist, väljatöötust, testimisdokumentatsiooni, standardeid vahendeid ja meetodeid. Selleks peaks IS audiitor saama auditi juhtkonnalt piisava koolituse ja juhendamise.	
	Teha koostööd IS personaliga spetsiifilise teabe hindamisel, sealhulgas terminoloogia alal ning juhtimiseesmärkide saavutamise spetsiifiliste vahendite ja meetodite osas.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

Projekti metoodika raamstruktuur	Organisatsiooni üldine eesmärk on rajada üldine projektihalduse raamstruktuur projekti haldamiseks kogu ta elutsükli kestel. See raamstruktuur peaks hõlmama vähemalt kohustuste jaotust, töö liigendust, aja ja ressursside eelarvestust, tähtpunkte, kontrollpunkte ja kinnitamisi. Teha kindlaks, kas projekti halduseks ja seireks on loodud projektihalduse metoodika raamstruktuur. See raamstruktuur peaks hõlmama vähemalt projekti käsitlusala, kohustuste jaotust, töö liigendust, aja ja ressursside eelarvestust, tähtpunkte, kontrollpunkte ja kinnitamisi. Arutada projekti metoodikat projektijuhiga ja teha kindlaks, millist SDLC metoodikat järgitakse. Kui juhtkond on kinnitanud mingi SDLC metoodika ja selle kasutamist nõudva poliitika, selgitada välja, kas seda SDLC metoodikat järgitakse. Kui ei järgita, teha kindlaks põhjused, miks ei kasutata kinnitatud metoodikat.	
	Teha kindlaks, kas järgitava metoodikaga hõlmatakse alljärgnev: projekti käsitlusala ja piiride dokumentatsioon, kohustuste jaotus, töö liigendus, aja ja ressursside eelarvestus, projekti tähtpunktid, kontrollpunktid, kinnitamisprotsess, riski kaalutlemise ja vähendamise protseduurid, suhtluse haldus.	
	Süsteemi arengu elutsüklis osaleb aktiivselt ärijuhtkond (huvipooled/projekti sponsorid). Kontrollida, kas ärijuhtkond vaatas läbi ja kinnitas ärialased nõuded ja projekti käsitlusala, kinnitas projekti eelarve ja seirab seda aktiivselt, saab projekti seisu protokolle ja/või osaleb projekti seisu ajakohastamistel, osaleb aktiivselt oluliste probleemide lahendamises.	
	Projekti hoidmiseks kontrolli all kogu ta eluea kestel koostatakse projekti üldplaan. Teha kindlaks, kas projekti üldplaan on dokumenteeritud; projekti plaan on kooskõlas tulude ja kulude analüüsiga, ajahinnangutega ja projekti tarneobjektidega; juhtkond on projekti plaani kinnitanud; projekti muudatuste kajastamiseks uuendab projektijuht plaani pidevalt projekti eri punktides; plaaniga on hõlmatud aspektid, mida käsitleb ülalnimetatud metoodika, ja järgnev: - lõpetamise kriteeriumid ja mõõdud, - kriitilise tee vastastikused sõltuvused, - iga töö eeldatav alustus- ja lõpetuskuupäev, - igale tööle määratud inimesed.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Projekti käigus tekkivate kulude seireks rakendatakse mingit metoodikat. Teha kindlaks, kas projekti eluea kestel tekkivate kulude seireks rakendatakse mingit protsessi; kas sellel protsessil on - protseduurid projekti kõigi kulude arvestuseks, - meetodid tegelike ja plaaniliste kulude võrdlemiseks.	
	Projektile liikmete määramise alus peab tagama, et kõik mõjutatavad alad on esindatud ja et projektirühmal on adekvaatsed teadmised. Peale selle peavad olema määratletud projektirühma liikmete kohustused ja õigused. Teha kindlaks, milliseid kriteeriume järgis juhtkond projektirühmade liikmete määramisel nii, et oleks tagatud projektirühma asjakohane ärialase ja tehnilise asjatundmise tase ning mida tehakse personali koolitamiseks ja/või asjatundmise saamiseks, kui personalil ei ole vajalikku asjatundmise taset; kas projektirühma kuuluvad nende alade esindajad, mida mõjutab projekt; kas projekti plaan spetsifitseerib selgelt projektirühma iga liikme rollid ja kohustused; kas rühma liikmed tunnevad oma rolle ja kohustusi; kas tarnija või kolmanda poole (kui on) rollid ja kohustused on selgelt määratletud.	
	Iga järgu tulemuste kinnitamiseks enne töö jätkamist järgmises järgus on nimetatud juhtkonna esindajad nii äritegevuse poolelt kui ka IT aladelt. Teha kindlaks, kas mõjutatava ala esindajad on nimetatud kinnitama järgu saadusi; projekti plaanis on sätted, mis nõuavad, et saadusi kinnitaksid selleks nimetatud ärialased töötajad, kvaliteedi tagamise töötajad ja IT töötajad.	
	Kvaliteedi tagamise sammud tuleks lülitada projekti üldplaani ning kõik pooled peaksid need formaalselt läbi vaatama ja kinnitama. Tagamistööd toetavad süsteemi akrediteerimist ja peaksid tagama, et sisemised meetmed ja turvafunktsioonid vastavad nendega seotud nõuetele. Teha kindlaks, kas kas projekti plaani läbivaatamisel on sinna lülitatud kvaliteedi tagamise sammud; kvaliteedi tagamise protsess sisaldab samme projekti saaduste läbivaatuseks väljatöötuse strateegilistes punktides, mõistliku kinnituse saamiseks sellele, et lõpptulemitega rahuldatakse või ületatakse - ärinõuded, - õiguslikud nõuded, - organisatsiooni standardid, - turvastandardid, - sisejuhtimise nõuded, - usaldatavusnõuded, - sooritusnormid; kvaliteedi tagamise plaani on võetud - probleemide jälgimine ja logimine, - muudatuste ja defektide jälgimine ja logimine, - üldise testimisstrateegia väljatöötamine.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Projektiga seotud riskide tuvastamiseks, kõrvaldamiseks või minimeerimiseks peaks olema rajatud formaalne riskihaldus. Teha kindlaks, kas projektirühm on tuvastanud ja dokumenteerinud projektiga seotud riskid; kas riskihalduse protsessi järgimiseks ja probleemide halduseks on olnud projekti seisu aruannete läbivaatus; projektijuhti küsitledes, milliseid samme on astutud teadaolevate projekti riskide vähendamiseks; kas riskidest on selgelt teatatud juhtkonnale.	
	Kasutusel peaks olema protsess projekti seisu usaldatavaks ja õigeaegseks teatamiseks juhtkonnale. See teatamismehhanism peaks hõlmama ka lahknevusi plaanist ja ilmnenud probleeme. Teha kindlaks, kuidas hinnatakse projekti seisu. Projekti tundmise põhjal vaatab IS audiitor läbi seisu aruanded ja/või osaleb seisu arutamise koosolekutel, et teha kindlaks, kas see hindamismehhanism on adekvaatne projekti täpse seisu teatamiseks juhtkonnale. Kontrollida, kas teatatakse ka lahknevustest plaani suhtes ja probleemidest; milline on juhtkonnale projekti seisu teatamise meetod ja ajastus ning kas teatamismehhanism on adekvaatne andma juhtkonnale usaldatavat ja õigeaegset teavet; kas on põhjalikke küsitlusi, kas juhtkond saab seisu aruandeid ja vaatab neid läbi ja/või osaleb seisu arutamise koosolekutel ja rakendab vajalikke meetmeid ning kas projektirühma kasutatav teatamismehhanism annab talle adekvaatset teavet; kas teatatakse muudatustest projekti plaanis ja/või lahknevustest plaani suhtes ning kas juhtkond osaleb probleemide lahendamises.	
	Peaksid olema rajatud protsessid, millega tagada kõigi projektis osalevate poolte vaheline tihe koordinatsioon ja suhtlus. Teha kindlaks, kas kõik projektirühma liikmed osalevad projekti koosolekutel asjakohasel tasemel ning kas neil koosolekutel osalevad IT, kvaliteediala ja äritegevusalade esindajad; millised formaalsed suhtluskanalid on loodud. Rühma liikmetega arutades teha kindlaks, kas suhtlus näib olevat õigeaegne ja toimiv; kas projekti dokumentatsiooni säilitatakse ja kas see on kõigile asjassepuutuvatele kättesaadav. Kontrollida, kas seda dokumentatsiooni saavad muuta ainult selleks volitatud isikud; kas (vastavalt vajadusele) on dokumenteeritud - projekti käsitlusala ja tulemsaadused, - tasuvuse ja teostatavuse uuringud, - riskianalüüs, - projekti organisatsiooniskeem, - projekti seis, - projekti plaan, - kasutaja nõuded, - lahenduse spetsifikatsioonid, - probleemide logid ja lahendused, - testimisstrateegia, - üleviimise metoodika, - evitusplaan, - koolitusplaan, - evitusjärgne läbivaatus; kas projektirühm on seotud tarnijaga või kolmanda poolega ning kas on loodud suhtluskanal mõistliku kinnituse saamiseks sellele, et kolmanda poole ja projektirühma vaheline suhtlus on toimiv.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Peaks olema loodud protsess parandusmeetmeid nõudvate probleemide tuvastamiseks ja neist teatamiseks. Teha kindlaks, kas on olemas protseduurid probleemide tuvastuseks, mõõtmiseks ja kõrvaldamiseks; milline mehhanism on olemas mõistliku kinnituse saamiseks sellele, et probleemid lahendab asjakohane isik õigel ajal; kas on olemas mehhanism juhtkonna õigeaegseks kaasamiseks oluliste probleemide käsitlusse; kas juhtkond vaatab läbi probleemide lahendused ja kinnitab need.	
	Teha kindlaks, kas kõik erandid dokumenteeritakse ja kas neist teatatakse juhtkonnale parandusmeetmete rakendamiseks. Parandusmeetmete dokumentatsioon peaks kuuluma auditi töömaterjalide hulka.	
Projekti algatamine (taotlus ja kinnitamine)	Üldeesmärk on selles, et organisatsioon peaks kasutama mingit metoodikat projektide piiritlemiseks ja neile prioriteetide andmiseks kooskõlas tegevusplaaniga. Teha kindlaks, kas kasutatav metoodika sisaldab mingit protsessi, millega hinnata ärinõudeid, projekti kulusid, võimalikke riske ja eeldatavaid hüvesid. Peale selle peaks tarkvara muudatuste taotluste loetelu olema tsentraliseeritud ning peaks näitama taotluste allikaid; need võivad olla näiteks äritegevuse omanik (strateegiliste lisafunktsioonide saamiseks), konsultatsioonipunkt (näiteks probleemiavalduste põhjal), taktikaline täiustamine (igapäevased väikesed muudatused) jt.	
	Projekti määratlemises ja volitamises peaksid osalema kõigi mõjutatavate ärialade ja IT-alade esindajad. Teha kindlaks, kas projekti hindamiseks loodud rühma kuuluvad kõigi mõjutatavate ärialade ja IT-alade esindajad; neil esindajail on selle ülesande täitmiseks vajalikud äritegevuse alased ja/või tehnilised teadmised. Teha kindlaks, kas vajaduse korral kasutatakse teadmuse täiendamiseks eriala asjatundjaid.	
	Projekti iseloom ja käsitlusala peaks olema selgelt kirjalikult määratletud, nii et juhtkond saaks enne projekti algatamist projekti kinnitada; see aitab tagada, et projekt vastab ärinõuetele ja strateegilisele suunale. Teha kindlaks, kas projekti taotlus tuli volitatud allikast ja on kooskõlas äristrateegia suunaga; projektile on määratletud üldised ärialased ja käituslikud nõuded (näiteks oodatav käideldavus), sealhulgas - oodatavad hüved ja/või ärialane põhjendus, - üldised ärialased nõuded, - ärialad ja -süsteemid, mida projekt eeldatavalt mõjutab, - oodatav klientuur, - süsteemi käideldavusaspektid, - süsteemi eeldatav maht, - oodatav reaktsiooniaeg, - ootused taaste suhtes, - kasutuskõlblikkuse nõuded, - õigusliku ja muu vastavuse nõuded; projekti käsitlusala on selgelt määratletud, käsitlusala dokumentatsioon määratleb projekti piirid ning määrab konkreetselt, mis tuleks hõlmata projektiga ja mis mitte; projektinõudeid on hinnatud mõistliku kinnituse saamiseks sellele, et nad toetavad äriüksuse strateegilist suunda ja ettevõtte strateegilist suunda.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Tuleks välja selgitada alternatiivsed ärinõudeid rahuldavad lahendused. See aitaks tagada optimaalse lahenduse valimise. Teha kindlaks, kas järgiti mingit protsessi mõistliku kinnituse saamiseks sellele, et arvessevõtuks selgitati välja kõik äriprobleemi võimalikud lahendused; on võetud arvesse järgmised lahendused: - senise süsteemi täiustused, - käsioperatsioonid ja/või ajutised hädamuudatused, - tarnijate lahendused, - kavandamine ja väljatöötamine oma jõududega; iga lahendust on hinnatud selle põhjal, kui hästi ta võiks rahuldada ärinõudeid; järeldused iga väljaselgitatud lahenduse kohta on dokumenteeritud ja kas on tuvastatud need, mida valida edasiseks uurimiseks ja analüüsiks.	
	Projekti jätkamise otsuse alusena tuleks hinnata iga alternatiivi teostatavust. Teha kindlaks, kas on sooritatud iga pakutud lahenduse teostatavuse analüüs ja kas selle uuringu tulemused on juhtkonna jaoks dokumenteeritud; teostatavuse analüüs hõlmab ka olulise personali olemasolu, sealhulgas - ärialast personali, - kvaliteedi tagamise personali, - tehniliselt oskuslikku arenduspersonali; lahenduse teostamiseks vajalikud tähtajad on projektinõuetega spetsifitseeritud tähtaegade piirides, tarkvara ja riistvara on analüüsitud mõistliku kinnituse saamiseks sellele, et - praegune tehnoloogia toetab projekti, - organisatsioon toetab seda tehnoloogiat, - see tehnoloogia on kooskõlas organisatsiooni tehnilise strateegia ja arhitektuuriga.	
	Projekti jätkamise otsuse alusena tuleks hinnata iga alternatiivi tasuvust. Kulusid ja hüvesid tuleks uurida rahalises ja mitterahalises väljenduses. Rahalised kulude säästud ja tulud peaksid olema mõõdetavad, saavutatavad ja kontrollitavad. Teha kindlaks, kas on sooritatud iga pakutud lahenduse tasuvuse analüüs ja kas selle tulemused on juhtkonna jaoks dokumenteeritud; tasuvusanalüüsiga on hõlmatud kõik otsesed, kaudsed, vähenevad ja korduvad kulud: - tööjõukulud, sealhulgas infrastruktuuri- ja käituspersonalile, alltöövõtjaile, väljatöötajaile, kvaliteedi tagamise personalile ja ärialasele personalile, kes on kinnistatud projektile; - iga-aastased litsentsi- ja lepingutasud; - kulud, mis on seotud täiendite installeerimisega riistvara ja tarkvara hoidmiseks hetketasemetel ja/või süsteemi hoolduseks ta eluea kestel; - riistvarakulud (sealhulgas kulum); - koolitus; tasuvusanalüüsiga hõlmatakse projekti hüved, sealhulgas - ajasäästud, - tööjõusäästud; - riistvara ja/või käituse säästud, - oodatavad tulude tõusud ärialaste hüvede tõttu (näiteks: uus äritegevus, suurem klientuur). Vaadelda selle ürituse tasuvust, et teha kindlaks, kas tuvastatud kulud ja tulud näivad olevat mõistlikud, mõõdetavad ja saavutatavad. Teha kindlaks, kas arvutused tunduvad olevat mõistlikud. Kas kulude ja tulude analüüs hõlmab süsteemi realistlikku eluiga (näiteks viit aastat) ja kas ta arvestab tehnoloogia vananemist?	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Projektiga seotud riskide tuvastamiseks, kõrvaldamiseks või minimeerimiseks sooritatakse riskihaldust. Teha kindlaks, kas iga võimaliku alternatiivi kohta on sooritatud riski kaalutlemine ning kas projekti eeldused ja projekti riskid on dokumenteeritud ja juhtkonnale teatavaks tehtud; juhtkond on välja töötanud võimalikud lahendused teadaolevate riskide vähendamiseks.	
	Projektile kõigi ressursside eraldamise tagamiseks peaks projekti kinnitama juhtkonna asjakohane tase. Teha kindlaks, kas juhtkond on projekti dokumentatsiooni läbi vaadanud ning teab projekti käsitlusala, teostatavust, tasuvust ja riski; kinnitanud projekti eelarve ja kas see kinnitus sisaldab tähtpunkte projekti edenemise hindamiseks; võtnud endale kohustuse olla selle projekti omanik ja vastutuse projekti eest..	
	Teha kindlaks, kas kõik ootused on dokumenteeritud ja neist on teatatud juhtkonnale parandusmeetmete rakendamiseks. Parandusmeetmete dokumentatsioon tuleks võtta auditi töödokumentide hulka.	
Ärinõuete määratlemine	Üldeesmärk on see, et organisatsioon peaks kasutama mingit metoodikat, mis tagab ärinõuete määratlemise ja dokumenteerimise projekti üldeesmärkide toetamiseks.	
	Ärinõuete väljatöötamises peaks osalema asjakohane personal. Kontrollida, kas ärinõuete määratlemises osalevad kõik projektiga mõjutatavad äritegevuse alad; personalil on ärinõuete määratlemiseks adekvaatsed teadmised.	
	Ärinõuded olgu selgelt dokumenteeritud ning täpsed, täielikud ja ajakohased. Kontrollida, kas projektirühm on käsitlenud kõiki ärinõudeid; projektijuht või IT-juht on korraldanud üksustevahelise nõupidamise teiste IT-alade ja äritegevuse omanikega, et hinnata tarkvara muudatuse mõju nende tööülesannetele. Neid nõupidamisi tuleks protokollida ning väljaselgitatud mõjusid tuleks arvestada nõuetes ja lahenduses. Selle nõude või meetme puudumise tulemuseks võib olla negatiivne mõju teistele allüksustele või kavandamise toimivuse kadu; ärinõuded on dokumenteeritud ja nende hulka on võetud - funktsionaalsed ja tehniliste protsesside nõuded, - õigusalased nõuded, - turvanõuded, - liidestusnõuded, - ajastusnõuded ja nõuded reaktsiooniajale, - aruandlusnõuded, - nõuded sisendmaterjalile, - auditeerimisnõuded; projektirühm on taganud lõplike ärinõuete teatavakstegemise kasutajaile ja juhtkonnale; äririskid on tuvastatud ja neid arvestatakse ärinõuetes.	
	Probleemihalduse küsimused tuleks tuvastada, logida ja lahendada. Teha kindlaks, millist meetodit kasutatakse ärinõuete väljatöötamisel tuvastatud probleemide arvelevõtuks ja logimiseks; kas probleemid on analüüsitud ja lahendatud.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Tuleks kasutada mingit metoodikat, millega tagada kõigi potentsiaalsete tarnija toodete arvessevõtt ja hindamine ärinõuete põhjal. Teha kindlaks, kas on välja töötatud meetod potentsiaalsete tarnijate ja toodete hindamiseks; milline tarnija rahalise stabiilsuse analüüs tehti; kuidas hinnati klientide rahulolu tarnijatega; kas pakkumiskutse protsess oli loogiline ja põhines tootel, hinnal, tehnilisel platvormil, usaldatavusel, tarnija mainel ja ärinõuetele vastavusel; kas tarnijate vastuseid pakkumiskutsele hinnati ühiste kriteeriumide (näiteks ärinõuete) põhjal.	
	Suhteid tarnijatega ja lepinguid nendega tuleks asjakohaselt hallata. Kontrollida, kas lepingud tarnijatega on läbi vaadanud jurist; lepingud kolmandatega on läbi vaadanud ja kinnitanud tarnija juhtkond ja ärijuhtkond; lepinguga on hõlmatud - konkreetsed mõõdetavad tarneobjektid, - maksete ajakavad, - trahvid saaduse tarne hilinemise või ärajäämise eest, - konkreetsed kohustused tehnilise ja kasutajadokumentatsiooni ning koolituse alal, - tarkvaras tehtavate muudatuste (kui neid on) määratlused, - muudatuste halduse kriteeriumide selge esitus, - lepingu käsitlusalas sisalduva ja sellest välja jääva määratlus, - väljaspool lepingut lisatsu eest sooritatavate tööde spetsifikatsioonid ja nende eest tasumise alused (püsitariif, aeg ja materjalid vms), - süsteemi hooldamise kohustused, ajakohastamise sagedus ja tariifid; leping käsitleb lähtekoodi hoiustust; lepingus on asjakohane konfidentsiaalsuslepe.	
	Tuleks sooritada ärinõuete formaalne läbivaatus ja kinnitamine. Teha kindlaks, kas formaalne läbivaatus toimus ja tulemused dokumenteeriti, formaalse läbivaatuse protsessis osalejad esindavad äriala kõiki tahke, nii et kõiki ärinõudeid saab õiglaselt hinnata.	
	Tarkvara muudatuse eesmärkide mõistmiseks vaadata läbi IT strateegiad ja poliitikad (st oma väljatöötus, kolmandate lahendused, parim valmistoode, individualiseerimiseta) mõistliku kinnituse saamiseks sellele, et audit on keskendatud asjakohaselt ning IS audiitor otsib õigeid meetmeid.	
	Teha kindlaks, kas kõik erandid on dokumenteeritud ja neist on juhtkonnale teatatud parandusmeetmete rakendamiseks. Parandusmeetmete dokumentatsioon tuleks võtta auditi töödokumentide hulka.	
Süsteemi kavandamine ja väljatöötamine	Üldine eesmärk on selles, et süsteemi lahendus oleks täielikult määratletud ja dokumenteeritud ning lõplikud spetsifikatsioonid oleksid enne täieulatuslikku väljatöötamist läbi vaadatud ja kinnitatud, mõistliku kinnituse saamiseks sellele, et spetsifikatsioonid vastavad kasutaja nõuetele. Märkus. On soovitatav, et selle töölõigu sooritaks IT- ja ärialastest siseaudiitoritest koosnev töörühm. Audiitorid peaksid tuvastama kavandatava rakenduse olemuslikud äririskid. Mõistliku kinnituse saamiseks sellele, et vaadeldavas järgus on kavandatud meetmed nende riskide käsitluseks, tuleks läbi vaadata süsteemi lahenduse dokumentatsioon.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Kasutusel peaks olema protsess, millega tagada, et lahenduse spetsifikatsioonid on dokumenteeritud piisavalt detailselt, nii et neid saaks väljatöötajaile adekvaatselt esitada. Teha kindlaks, kas lahenduse spetsifikatsioonid on põhjalikult dokumenteeritud. Detailspetsifikat-sioonides peaksid olema muuhulgas järgmised andmed: - süsteemi turvanõuded, - süsteemi vooskeemid, - süsteemi riistvara spetsifikatsioonid ja nõuded lahendusele, - kuvade spetsifikatsioonid (sh kuva redigeerimine ja turvastsenaariumid), - liideste määratlused (sh täielikkuse ja redigeerimise kontroll), - failide ja andmebaaside lahendus, - nõuded süsteemi ajakohastusele, arvutustele ja töötlusele, - ajalooliste andmete talletus ja konversioon, - aruannete spetsifikatsioonid (sh sagedus ja printimiskoht), - nõuded lähtedokumentidele, - programmide spetsifikatsioonid, - süsteemi sise- ja välisliidesed, - süsteemi või rakenduse auditeerimisnõuded; kas seoses süsteemi lahendusega on kavandatud ja dokumenteeritud käsiprotseduu-rid, mõistliku kinnituse saamiseks sellele, et - saab tagada adekvaatse kohustuste lahususe, - on välja töötatud adekvaatne kinnitusprotsess, - on kavandatud veaparanduse protseduurid, - on välja töötatud süsteemi tasakaalustuse protseduurid.	
	Lahenduse spetsifitseerimise protsessis peaks osalema asjakohane personal. Teha kindlaks, kas lahenduse spetsifitseerimises osaleval personalil on adekvaatsed teadmised ja erialad (on näiteks ärivaldkonna asjatundja, andmebaasihaldur, võrguspetsialist); kavandamisprotsessis osaleb esindaja igalt süsteemiga mõjutatavalt alalt.	
	Detailprojekteerimise käigus kerkivate probleemide tuvastuseks, arvelevõtuks ja lahendamiseks tuleks rakendada mingit protsessi. Teha kindlaks, kas on kasutusel protsess detailprojekteerimise ajal kerkivate probleemide jälgimiseks; kas probleemide lahendamises osalevad asjakohased inimesed; kas probleemide lahendused on dokumenteeritud ja asjakohaselt teatavaks tehtud kogu rühmale, eriti programmide väljatöötajaile, kes peavad teostama muudatused; kas probleemide lahendused on läbi vaadatud, mõistliku kinnituse saamiseks sellele, et ärivajadused on endiselt rahuldatud ja lahendused on projekti käsitlusalas.	
	Tuleks kavandada protseduur lähtedokumentide halduseks. Teha kindlaks, kas lähtedokumentide halduse lahendusega on hõlmatud - säilituse tehnoloogia, - säilitustavad, - lähteteabe võtu võime, - täielikkuse ja õigsuse kontrollimise protsess; lähtedokumentide teabe vastuvõtuks, kinnitamiseks ja sisestuseks kavandatud protsess tagab adekvaatse kohustuste lahususe; lähtedokumentatsiooni käsitluse protsess oma praegusel kavandatud kujul vastab õigusaktide nõuetele.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Tuleks määratleda, dokumenteerida ja valideerida andmete käsitsi sisestamise meetodid. Teha kindlaks, kas sisestuse spetsifikatsioonid hõlmavad sisestatavate andmete redigeerimist; on kavandatud protseduurid vigade tuvastuseks, teatamiseks ja/või parandamiseks; projektirühm on välja töötanud mingi kuvastandardi, mõistliku kinnituse saamiseks sellele, et - kogu süsteemis on ühesugune tööilme, - üldised funktsioonid, näiteks organisatsiooni logo või kaubamärgi esituse, funktsiooniklahvide otstarbe, lehe- ja reakerimise meetodi jms on ühtsed, - kuvad on läbi vaadatud kasutuskõlblikkuse ja kasutajasõbralikkuse seisukohalt; süsteemi lahendusse on võetud sisespikker.	
	Peaksid olema määratletud ja dokumenteeritud töötlusnõuded süsteemi liidestele (sisestusele ja väljastusele). Teha kindlaks, kas on dokumenteeritud reeglid või protseduurid tulemuste kooskõlastamiseks programmide, tööde või liideste vahel; juhul, kui süsteemi lahendus sisaldab olemasolevate süsteemide või liideste muudatusi, asjakohane uue süsteemiga mõjutatavate süsteemide personal vaatab need muudatused läbi ja kinnitab need; liidese tõrke puhuks on kavandatud poliitikad ja protseduurid probleemi käsitluse laiendamiseks ja probleemi lahendamiseks.	
	Peaksid olema koostatud ja dokumenteeritud andmete määratlused ja andmenõuded. Teha kindlaks, kas projekti spetsifikatsioonides on teavet failivormingute, andmesõnastike ja andmevooskeemide kohta; kas süsteemi iga faili ja andmebaasi kohta on esitatud järgmised andmed: - nõuded andmete talletusele, - varunduse strateegia, - turvanõuded; kas vajatakse andmebaaside spetsialisti. Kontrollida andmebaasihalduriga, kas andmebaasi üldlahendust on hinnatud liiasuse ja andmetervikluse seisukohalt; kas nähakse ette andmete konversiooni, kas on kavandatud ja dokumenteeritud konversiooni strateegia ning kas selle strateegiaga määratakse - lähtesüsteemi andmete läbivaatus nende täielikkuse ja õigsuse seisukohalt, - protsess, millega juhtkond saab sisestuskontrolli, viitetervikluse kontrolli, kirjete loenduse ja kontrollsummade abil kontrollida, kas elektrooniliselt konverteeritud teave on täielik ja õige, - protsess, millega juhtkond saab kontrollida, kas andmete käsitsi sisestamisel uude süsteemi on andmed täielikud ja õiged; kas juhul, kui rakendus on mingi valmispakett, mis nõuab tarkvara talitluse juhtimiseks mingite andmespetsiifiliste parameetrite sisestust, on need valitavad parameetrid dokumenteeritud.	
	Püsiandmete töötlus, ajakohastamine ja hooldus peaks olema määratletud ja dokumenteeritud. Kontrollida, kas talitlusreeglid, nõuded ja töövood on määratletud; programmide detailspetsifikatsioonid on koostatud ja vastavad äritalitluse spetsifikatsioonidele; on kavandatud kooskõlastusprotseduurid (st sisemise kooskõlastuse rutiinid), mõistliku kinnituse saamiseks sellele, et püsiandmeid hooldatakse õigesti; äritegevuse omanik kinnitab püsiandmete aruanded nende täielikkuse tagamiseks.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Väljastuse ärinõuded peaksid olema määratletud ja dokumenteeritud. Teha kindlaks, kas lahenduse spetsifikatsioonid hõlmavad väljundfailide ja -vormingute dokumentatsiooni, aruandeid ja dokumente (näiteks tšekke või organisatsiooni deklaratsioone). Kontrollida, kas on käsitletud järgnev: - väljastuse sagedus, - väljastuse turve, - printimiskoht ja printdokumentide jaotamine; on määratletud reeglid väljundtulemite kooskõlastuseks, on määratletud protseduurid vigade ja probleemide tuvastuseks, seireks, teatavakstegemiseks ja kõrvaldamiseks.	
	Määratletud ja dokumenteeritud peaksid olema nõuded süsteemi arhitektuurile. Kontrollida, kas süsteemi personal on arvestanud arhitektuuri lahenduses kõiki tehingumahte, kasutajate arvu, oodatavat reaktsiooniaega ja üldist sooritusvõimet; arhitektuur on kooskõlaline ja ühildub organisatsiooni infrastruktuuriga; on arvesse võetud muud kitsendused, näiteks - aruandlusnõuded, - pakktsüklid, - varundusnõuded, - andmevood teistesse süsteemidesse ja teistest süsteemidest, - süsteemi käideldavusnõuded, - süsteemi ja riistvara hooldus, - süsteemi kasv (tehingute maht ja kasutajate arv), - süsteemi hooldus ja tsüklilised ajakohastused; süsteemi arhitektuur ühildub andmebaasi ja programmide lahendusega.	
	Kavandatud ja dokumenteeritud peaks olema mingi strateegia turbe rakendamiseks süsteemi ja rakenduste ressurssidele. Kontrollida, kas on kavandatud ja dokumenteeritud loogiline ja füüsiline turve riistvara ja süsteemitarkvara kaitseks; on kavandatud ja dokumenteeritud lähte- ja objektkoodi loogiline turve; on kavandatud ja dokumenteeritud rakenduste failide ja andmebaaside loogiline turve; rakenduste funktsioonide turve on määratletud ja tagab adekvaatse kohustuste lahususe.	
	Süsteemi lahenduse läbivaatamiseks peaks olema kasutusel kvaliteedi tagamise protsess. läbi vaadata süsteemi lahendus, et teha kindlaks, kas süsteemi koostisse on kavandatud adekvaatsed kontrolljäljed; kas on kavandatud sisemeetmed tuvastatud äririskide minimeerimiseks ja/või kõrvaldamiseks; mõistliku kinnituse saamiseks süsteemi andmete täielikkusele ja õigsusele on kavandatud adekvaatsed kooskõlastamise ja veatöötluse protseduurid; süsteem kavandatud kujul vastab õigusaktide nõuetele; süsteem kavandatud kujul vastab organisatsiooni standarditele, sealhulgas turvapoliitikatele ja infrastruktuuristandarditele; kavand arvestab kõiki eelmise ärialase lahenduse meetmete nõrkusi.	
	Mõistliku kinnituse saamiseks sellele, et süsteemi lahenduse spetsifikatsioonid vastavad ärinõuetele ning need on heaks kiitnud juhtkond, lõppkasutaja esindajad ja projektiga mõjutatavad alad, tuleks lõplikud spetsifikatsioonid läbi vaadata. Kontrollida, kas arendusrühm ja äritegevusala on lahenduse põhjalikult läbi uurinud mõistliku kinnituse saamiseks sellele, et lahendus on täielik ja vastab ärinõuetele; juhtkond on süsteemi kavandi spetsifikatsioonid läbi vaadanud ja kinnitanud ning tunneb neid.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Lähtekoodi ja objektkoodi halduseks arenduskeskkonnas peaksid olema välja töötatud protseduurid.Teha kindlaks, kas on olemas mingi protseduur lähtekoodi halduseks; kas on välja töötatud ja dokumenteeritud strateegia lähtekoodi halduse ja versiooniohje koordineerimiseks (näiteks versiooniohje instrument) väljatöötuse ja testimise järkudes; kuidas tarnija haldab lähtekoodi, ja teha kindlaks, kuidas projektirühm hakkab haldama objektkoodi, kui rakendus on ostetav süsteem; kas juurdepääs tootmisteekidele, kus asuvad rakenduse lähtekood ja talletatavad protseduurid, on ainult neil, kellel on selleks tööalane vajadus. Kui tarkvara muudatused nõuavad muudatusi andmebaasi struktuuris, tuleks saada mõistlik kinnitus ka sellele, et juurdepääs andmebaasi päästikutele on turvatud ja on üks osa sellest SDLC protsessist, mis hõlmab ka versiooniohjet.	
	Peaks olema kavandatud ja testitud mingi testimise keskkond või infrastruktuur. Teha kindlaks, kas uue rakenduse testimise toeks on kavandatud ja rajatud mingi testimiskeskkond; kas see keskkond on eeldatava tootmiskeskkonna koopia. Kui ta seda ei ole, tuvastada erinevused ja nende võimalik mõju testimistulemuste valiidsusele.	
	Süsteemi ja programmide dokumenteerimise standardid peaksid olema dokumenteeritud, IT personalile teatavaks tehtud ja kehtestatud. Kontrollida, kas on kehtestatud dokumentatsiooni loomise, hoolduse ja talletuse protseduurid või standardid. Vaadata läbi kogu seni koostatud dokumentatsioon (näiteks vooskeemid, andmevooskeemid, andmesõnastikud ja kirjete vormingud); kas lähtekoodi dokumenteerimise standardid annavad mõistliku kinnituse sellele, et programmid on isedokumenteerivad ja dokumenteerimiskohustuslikud; kas projekti plaanis on dokumenteerimisele eraldatud tähtajad; millist dokumentatsiooni peab andma ja/või hooldama tarnija, kui rakendus on ostetav süsteem. Teha kindlaks, kes hakkab hooldama kohandavate koodimuudatuste dokumentatsiooni.	
	Teha kindlaks, kas kõik erandid on dokumenteeritud ja parandusmeetmete rakendamiseks juhtkonnale teatavaks tehtud. Parandusmeetmete dokumentatsioon tuleks võtta auditi töödokumentide hulka.	
Testimine	Üldeesmärk on selles, et on määratletud, dokumenteeritud ja rakendatud mingi testimismetoodika mõistliku kinnituse saamiseks sellele, et väljatöötatud lahendus vastab määratletud ärinõuetele, vastab tehnilistele nõuetele, tuleb toime eeldatava tehingumahuga ja reaktsiooniajaga, annab õigeid tulemusi ja töötab usaldusväärselt.	
	Mõistliku kinnituse saamiseks sellele, et süsteemi funktsioonid testitakse täielikult, peaks testimisüksuse halduseks ja seireks olema kasutusel testimisplaan või -metoodika. Teha kindlaks, kas testimisplaan on olemas ja dokumenteeritud; kas testimise sooritamise ajakava on koostatud ja dokumenteeritud; kas testimiskriteeriumid on selgelt määratletud ja dokumenteeritud; kas on välja töötatud, määratletud ja dokumenteeritud täielikud testimisjuhud. Teha kindlaks, kas on olemas mingi viitemaatriks (näiteks jälitusmaatriks), mis seab iga konkreetse nõude vastavusse ametlikus üksikasjalikus ja dokumenteeritud "nõuete dokumendis", mille on koostanud ja/või kinnitanud äritegevuse omanik, ja tegelikes testimisplaanides. Kui sellist viitemaatriksit ei ole, hankida juhtkonnalt tuge ja dokumentatsiooni selle kohta, kuidas kontrollitakse seda, kas kõiki nõudeid testitakse; kas testimisplaan määratleb testimistulemuste läbivaataja ja kinnitaja; kas probleemide lahendamiseks on olemas protseduurid ja kas nad on mõistlikud; kas sisenemise ja väljumise strateegiat testitakse; milline on testimise käigus tuvastatud tuvastatud probleemide lahendamise ja intsidentide käsitluse kestus.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Testimisplaan koostatakse enne testimise alustamist. Vaadata testimisplaan läbi, et teha kindlaks, kas testimisplaan käsitleb adekvaatselt rakenduse kõiki funktsioone (st ärinõudeid). Testimisplaaniga peaksid olema hõlmatud - andmete sisestus, - redigeerimine (teated positiivsete ja negatiivsete kohta), - aruanded (sealhulgas prindi ja jaotamise käsitlus); - ajakohastused, arvutused ja töötlus; - veakäsitlus ja veateated, - liidesed, - turbefunktsioonid, - meetmed mõistliku kinnituse saamiseks sellele, et andmed on täielikud, õiged ja liiasuseta, - rakenduse kontrolljäljed ja süsteemi kontrollimehhanismid; testimisplaanis on arvessse võetud tehnilised komponendid, sealhulgas - jõudluse testimine, - pingustestimine (sealhulgas prindi puhul), - mahttestimine (normaalmahtudega ja suurimate prognoositud mahtudega tippaegadel), - võrgu stabiilsus; juhtkond simuleerib testimist tootmiskeskkonnas või sellele sarnanevas keskkonnas; juhtkond seirab testimisprotsessi, veendumiseks, et järgitakse testimismetoodikat.	
	Kogu testimisprotsessi kestel peaks olema kasutusel mingi protseduur muudatuste (sealhulgas vigade parandamise) halduseks. Teha kindlaks. millised protseduurid on kasutusel vigade käsitluseks, muudatuste halduseks ja probleemide lahendamiseks; probleemide tuvastamise, teatavakstegemise, seire ja jälgimise meetodid; kas juhtkond osaleb probleemide käsitluse laiendamises ja selliste muudatuste tegemises, mis võivad mõjutada süsteemi käsitlusalas või funktsioone; kas probleeme jälgitakse määratletud metoodika järgi; kas muudatuste käsitluseks on kasutusel standardid.	
	Mõistliku kinnituse saamiseks sellele, et programme hallatakse asjakohaselt, peaks olema kasutusel mingi protseduur tarkvara halduseks. Kontrollida, kas on loodud testimisteegid ja kas testimisele kuuluvaid programme talletatakse teekides; kellel on programmide lisamiseks, kõrvaldamiseks ja muutmiseks juurdepääs testimisteekidele; kas järgitakse protseduure tarkvara halduseks ja koodivarade halduseks (CAM); kas mitme programmeerija tehtavaid muudatusi programmides hallatakse nii, et ei kirjutata üle koodi, mille on kirjutanud ja testinud teised programmeerijad; kas on kasutusel mingi meetod mõistliku kinnituse saamiseks sellele, et uuesti testimiskeskkonda viidavaid muudatusi ohjatakse ja täielikult uuesti testitakse; kas pärast koodimuudatuste tegemist testitakse kõik funktsioonid uuesti.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Testimiseks tuleks luua eraldi keskkond. Teha kindlaks, milline testimiskeskkond on loodud kõigi testimisjärkude sooritamiseks, nii et oleksid hõlmatud - alusvariandi testimine, - üksuse testimine, - süsteemi testimine, - integratsiooni testimine, - rööptestimine, - regressioontestimine, - vastuvõtutestimine; mida on ette võetud testimiseks sisemiste ja väliste süsteemidega; kas testimiskeskkond on adekvaatne täiemahuliseks testimiseks, mis kajastab tegelikku tootmiskeskkonda; kas testimiskeskkonna tehniliste komponentidega tagatakse jõudluse testimine, pingustestimine (sealhulgas prindi puhul), mahttestimine (normaalmahtudega ja suurimate prognoositud mahtudega tippaegadel) ja võrgu stabiilsus.	
	Testimisnõuete taset tuleks hinnata ja katvus peaks vastama sellele hindamisele. Teha kindlaks, kuidas muudatused viiakse testjuhtudesse, dokumenteeritakse ja testitakse, ning kontrollida, kas alates testjuhtude väljatöötamisest ning lõpetades testimistulemuste läbivaatuse ja kinnitamisega, on testimisel esindatud kõigi testimisobjektiga mõjutatavate ärialade töötajad; projektirühm tagab kõigi võimalike süsteemi funktsioonide, tehingute, andme-kombinatsioonide ja veastsenaariumide hõlmamise testimisega; testimisega on hõlmatud kuulõpu, kvartalilõpu ja aastalõpu nõuded protsessidele ja andmetele; kõik testjuhud ja oodatavad tulemused on dokumenteeritud; kõik testjuhud on seotud ärinõuetega ja kõigi ärinõuete kohta on testjuhud; kogu testimisprotsessi kestel säilitatakse testandmete terviklus; on kasutusel mingi meetod testimise lahknevuste ja järgnevate lahenduste jälgimiseks; testjuhtudesse on võetud võimalikud erandiprotsessi funktsioonid.	
	Testimisplaani tuleks võtta loogilise ja füüsilise turbe nõuded. Teha kindlaks, kas testimisjärgu tarbeks on loogilise ja füüsilise turbe funktsioonid määratletud ja kasutusel; kes haldab turvet testimisjärgu kestel; kas testimisel rakendatav turve hõlmab juurdepääsu kuvadele, funktsioonidele, andmetele ja aruannetele.	
	Protsess ja protseduurid peaksid tagama koolituse uute süsteemide alal, nii et kasutajad saaksid aktiivselt osaleda testimises. Teha kindlaks, kas tarnija annab lõppkasutajaile koolitust nii, nagu on määratletud testimisplaanis, ja selliste tähtaegadega, mis on määratud plaanis; kas oma jõududega väljatöötatavate süsteemide alal on välja töötatud koolitus; kas lõppkasutajaile antakse koolitusmaterjali; kas lõppkasutajaile antakse koolitus õigel ajal, nii et nad saavad aktiivselt osaleda testimistegevustes; kas projektirühma juhtkond tagab koolituse adekvaatsuse ja sobivuse, hankides lõppkasutajailt tagasisidet ja rakendades vajaduse korral parandusmeetmeid.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Kasutusel peaks olema mingi protsess lõpliku vastuvõtutestimise määratlemiseks ja läbiviimiseks ning juhtkonnalt kinnituse saamiseks. Kontrollida, kas kogu testimine toimus testimisplaani järgi; kas juhtkond vaatab läbi ja kinnitab testimistulemused nii, nagu on kirjas projekti plaanis või testimisplaanis kas tarnija ja ärijuhtkond on läbi vaadanud ja kinnitanud lepingud kolmandate pooltega; kas asjakohane juhtkond on kõik testimistulemused heaks kiitnud ja kinnitanud.	
	Kasutusel peaks olema protsess, millega tagada jõudluse optimeerimine, nii et saaks prognoosida uue ja tunduvalt muutunud tarkvara käituseks vajalikke inimressursse. Teha kindlaks, kas projekti plaan sisaldab koolitusjärku; kas on olemas mingi protsess soorituse seireks ja kas lõppkasutajad tulevad koormusega toime (kui tööd on liiga palju, on vaja lisada personali); kas on kasutusel mingid protseduurid juhendite ja/või sisespikrite ajakohastamiseks.	
	Dokumenteerida kõik testimistulemused. Kontrollida, kas kõik testimistulemused on dokumenteeritud, sealhulgas oodatavad tulemused, tegelikud tulemused ja vajaduse korral rakendatud parandusmeetmed.	
	Teha kindlaks, kas kõik erandid on dokumenteeritud ja juhtkonnale parandusmeetmete rakendamiseks teatavaks tehtud. Parandusmeetmete dokumentatsioon tuleks võtta auditi töödokumentide hulka.	
Evitamine	Evituse üldeesmärk on luua ja käitada süsteemi vastavalt plaanile, mõistliku kinnituse saamiseks süsteemi edukale üleviimisele tootmiskeskkonda.	
	Koolituse ja süsteemi dokumentatsioon peaks olema valmis enne evitamist. Teha kindlaks, kas kasutajad on koolitatud ja oma uutest kohustustest teadlikud enne evitamist; kasutajaile, käituspersonalile ja programmeerijaile on kättesaadav adekvaatne teatmematerjal, sealhulgas - kasutajajuhendid, mis võivad sisaldada talitlusreegleid ja töötlus- ja kooskõlastus-protseduure, lähteandmete töötlust, veaparandusprotseduure ning kokkuvõtet süsteemi väljundandmetest ja korraldusest; - käitusjuhendid, mis võivad sisaldada ebanormaalse lõpu protseduure, varunduse ajakava, pakktöötluse ajakava, liideste kirjeldusi ja protseduure, nõudetoimingute loendeid ja käsitluse laiendamise protseduure; - programmeerijajuhendeid, mis võivad sisaldada programmide listinguid ja kirjeldusi, kuvavorme, failide ja andmebaaside kirjeldusi, vooskeeme ja tööde loendeid või ajakavasid.	
	Enne evitamist tuleks määratleda ja välja töötada teenusetasemelepped ja käitusnõuded. Teha kindlaks, kas enne evitamist on tarnijaga või sisemiselt sõlmitud teenusetasemelepped ja/või kokku lepitud käitusnõuded; kas enne evitust on arvesse võetud järgmised käitusalased vajadused: - tugi (tarnija või oma) konsultatsioonipunktilt, - avariijärgse taaste ja jätkusuutlikkuse plaanimine, - (tarnija või oma) muudatuste haldus, - varunduse ajakava, - pakktöötluse ajakava (vajadusel), - liidese ajakava (vajadusel), - riistvara ja süsteemitarkvara korraline ja perioodiline hooldus.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Evitusplaan peaks olema dokumenteeritud, teatavaks tehtud ja kinnitatud. Teha kindlaks, kas enne evitamist on koostatud plaan sammhaaval üleviimiseks. Kontrollida, kas selles plaanis on kõik süsteemi evituseks vajalikud tööd, nende tähtajad, tööde vahelised sõltuvused ja iga töö sooritamiseks määratud isikud; kuidas tagab juhtkond järgustatud evituse puhul iga järgu lõpetamise ja kinnitamise enne järgmise evitusjärgu alustamist; kas plaani koostamises on osalenud kõigi süsteemiga mõjutatavate alade esindajad ja kas plaan sisaldab töid kõigil mõjutatavail aladel (mõjutatavad äritegevuse alad, tootmise juhtimine, süsteemi tarkvara- ja võrguspetsialistid, andmebaasihaldurid). See läbivaatus sisaldab väljalaske halduse protsessi hindamist, mõistliku kinnituse saamiseks sellele, et muudatused ei ole vastuolus muude (näiteks interakteeruvate süsteemide või infrastruktuuri elementide) muudatustega; kas plaan tehti teatavaks kõigile süsteemiga mõjutatavatele äritegevuse aladele ja tehnilistele aladele; kas juhtkond on plaani kinnitanud.	
	Tootmisse üleviimise otsuse kinnitamiseks ja teatavakstegemiseks peaks olema loodud mingi metoodika. Teha kindlaks, kas juhtkond veendub, et süsteem on valmis tootmiskasutuseks; milline on tootmisse üleviimise otsustamise protseduur, sealhulgas lõpliku otsuse eest vastutaja; kas on kasutusel mingi meetod mõistliku kinnituse saamiseks sellele, et kõiki süsteemiga mõjutatavaid alasid on teavitatud tootmisse üleviimise otsusest.	
	Evitusprobleemide teatavakstegemiseks ja lahendamiseks peaks olema dokumenteeritud ja teatavaks tehtud mingi protseduur. Kontrollida, kas evitusprobleemide teatavakstegemise ja lahendamise plaan on dokumenteeritud ja teatavaks tehtud kõigile süsteemiga mõjutatavatele pooltele (näiteks evituse konsultatsioonipunktid, käsitluse laiendamise protseduurid, teavituspuud); mõistliku kinnituse saamiseks sellele, et probleemide korral mõjutatakse tootmisotstarbelist töötlust minimaalselt, on välja töötatud mehhanism evitusprobleemide käsitluseks; on välja töötatud ja dokumenteeritud taganemise strateegia. Kontrollida, kes vastutab taganemisstrateegia otsuse rakendamise eest ja kas kriteeriumid taganemisstrateegia rakendamiseks on dokumenteeritud.	
	Tootmisandmete üleviimiseks ja konverteerimiseks peaks olema välja töötatud, dokumenteeritud ja kinnitatud mingi protseduur. Kontrollida, kas andmete üleviimine on evitusplaani ühe osana dokumenteeritud; juhtkond kontrollib, kas üleviimine ei ole mõjutanud andmeid ning kas uus ja vana süsteem on töödelnud õigesti, täielikult ja liiasuseta; andmete üleviimise protsess annab mõistliku kinnituse sellele, et kõik andmed on konverteeritud õigesti ja täielikult. Kui vigade ja/või andmetõrgete puhul tuleb andmeid sisestada käsitsi, teha kindlaks, kas meetod tagab kõigi vigade arvessevõtu ja süsteemi kooskõlastuse pärast sisestust vigade korral.	
	Lõplikult kinnitatud süsteemikoodi üleviimiseks tootmiskeskkonda peaks olema välja töötatud mingi protseduur. Teha kindlaks, kas on olemas mingi protseduur lõplikult kinnitatud süsteemikoodi üleviimiseks tootmiskeskkonda; kas lõpliku kinnitamise ja tootmise keskkonnad on turvalised; kas kasutatakse üleorganisatsioonilist koodivarade halduse protsessi.	
	Teha kindlaks, kas kõik erandid on dokumenteeritud ja meetmete rakendamiseks teatavaks tehtud juhtkonnale. Parandusmeetmete dokumentatsioon tuleks võtta auditi töödokumentide hulka.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

Evitusjärgne läbivaatus	Üldine eesmärk on selles, et tuleks sooritada evitusjärgne läbivaatus, millega teha kindlaks, kas projekt on rahuldanud kasutajate ootused ning jäänud eelarve ja tähtaegade piiridesse. Peale selle hõlmatakse evitusjärgse läbivaatusega protsesside terviklus, st äritegevuse sisemeetmete rakendamine süsteemis; rakenduste turve.	
	Juhtkond peaks kaaluma evitusjärgse läbivaatuse korraldamist projektiplaani järgimise kontrollimiseks. Teha kindlaks, kas on sooritatud evitusjärgne läbivaatus. Kontrollida, kas selle läbivaatusega hõlmati - eelarveliste ja tegelike kulude võrdlus ja lahknevuste seletus; - algse plaanilise ajakava ja väljatöötuse tegeliku ajakava võrdlus ja lahknevuste seletus; - algse käsitlusala ja üleantud süsteemi käsitlusala võrdlus ja lahknevuste seletus; aitamaks tulevastel projektirühmadel vältida vigade kordamist on dokumenteeritud või vähemalt projektirühmaga läbi arutatatud saadud õppetunnid ja ilmnenud õnnestumised.	
	Juhtkond peaks vaatama läbi, millises ulatuses on evitatud süsteem saavutanud projekti eesmärgid. Teha kindlaks, milline on meetod, mida juhtkond kasutab tagasiside saamiseks süsteemi õnnestumise või nurjumise kohta; kuidas juhtkond mõõdab seda, kas süsteemilt oodatavad hüved realiseeruvad; kuidas kavatseb juhtkond uurida ja lahendada ilmnenud lahknevusi ootuste ja süsteemi lõplike tarnesaaduste vahel; mil määral on kasutajad süsteemiga rahul. Kui kasutajad ei ole rahul, teha kindlaks nende rahulolematuse põhjused (näiteks: kuvad ei ole kasutajasõbralikud, reaktsiooniaeg on pikk, pole adekvaatset koolitust).	
	Evitusjärgsete probleemide seireks ja käsitluseks peaksid olema kasutusel mingid protseduurid. Teha kindlaks, kas on võetud kasutusele mingi protseduur evitusjärgsete probleemide jälgimiseks, prioriteetimiseks ja lahendamiseks; kas kasutajail on adekvaatsed ressursid probleemide lahendamiseks (näiteks konsultatsioonipunkt, erialaspetsialistid süsteemi alal); kas lõppkasutajate koolitus oli asjakohane ja võimaldab kasutajail süsteemi edukalt kasutada.	
	Süsteemi väljatöötamiselt süsteemi hooldusele ja tootmise toetamisele siirdumiseks peaks olema kasutusel mingi metoodika. Teha kindlaks, kas on kasutusel protseduurid rakendusele taotletud täiustuste jälgimiseks ja prioriteetimiseks (näiteks probleemi- või konsultatsiooniavaldused, formaalne projekti üleandmine, sealhulgas täitevjuhtkonnalt kinnituse saamine suurtele projektidele); kas on kehtestatud mingi protsess lähtekoodi halduseks; kas turvalisust mõjutavad õigused, mis võisid olla vajalikud süsteemi väljatöötamiseks ja evitamiseks, tühistatakse õigeaegselt; kas ostupaketi korral on müüja hooldusteenused selgelt määratletud; kas probleemi- ja konsultatsiooniavalduste käsitlus koos juurpõhjuse analüüsiga sooritatakse õigeaegselt (näiteks hädamuudatus tehakse 48–72 tunniga). Peale selle võib osutuda asjakohaseks rakenduse muudatustega seotud probleemide trendianalüüs.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Juhtkond peaks seirama uue süsteemi töötulemusi vähemalt kuni ühe tegevustsükli eduka sooritamise lõpuni. Kontrollida, kas juhtkond vaatab läbi sooritusaruanded, sealhulgas järgmised näitajad: reaktsiooniajad, tehingumahud, vead, süsteemi käideldavuse, tarnija töösoorituse.	
	Teha kindlaks, kas kõik erandid on dokumenteeritud ja parandusmeetmete rakendamiseks tehtud teatavaks juhtkonnale. Parandusmeetmete dokumentatsioon tuleks võtta auditi töödokumentide hulka.	
Plaaniväline hädamuudatus	Hädamuudatuste üldine eesmärk on nende vajaduse ajal lahendada süsteemi probleemid ja võimaldada elutägtsal töötluse jätkuda. IS audiitorid peaksid vaatama läbi selliste protseduuride olemasolu ja järgimise, mis annavad mõistliku kinnituse selle kohta, et hädaparandusi on võimalik sooritada süsteemi terviklust rikkumata. Teha kindlaks, kas on olemas hädamuudatuste protsess ja selle dokumentatsioon; kas hädamuudatused dokumenteeritakse ja kinnitatakse asjakohaselt; kas hädamuudatused enne nende püsivaks muutmist lõplikult testib ja vaatab läbi muudatuste ohje nõukogu; millise protsessiga kasutatakse ja seiratakse hädamuudatuste kasutajatunnuseid.	
	Mõnikord võidakse vajada hädamuudatusi süsteemi probleemide lahendamiseks ja elutähtsa töötluse jätkamise võimaldamiseks. Kontrollida, kas on olemas protseduurid mõistliku kinnituse saamiseks sellele, et hädaparandusi on võimalik sooritada süsteemi terviklust rikkumata, sooritades protsessist arusaamise kinnituseks hädamuudatuste ohje protsessi läbikõnni; dokumenteerides konsultatsioonipunkti vastustoimingud hädaolukordadele, mis võivad nõuda programmimuudatusi; tehes kindlaks, kas need muudatused töödeldi muudatuste ohje protsessi kaudu.	
	Meetmete haldus hõlmab hädamuudatuste protsessi, mida tuleks hallata nii, et standardsest muutmisprotsessist möödumine nõuaks kinnitust. Kontrollida, kas hädamuudatuse ajal toimuvad tegevused logitakse ja need vaatab läbi juhtkond koos rakenduse väljatöötajate rühmaga ja turvateenuste rühmaga (näiteks suurte õigustega kasutajatunnuse tõttu, mis anti programmeerijale süsteemi käideldavust taastava hädamuudatuse tegemiseks); pärast süsteemi tagastamist kasutamiseks kliendile kõrvaldatakse programmeerija juurdepääs tootmiskeskkonnale, tehakse täielik tõrkejärgne analüüs koos juurpõhjuse analüüsiga ja sooritatakse regressioontestimine selgitamaks välja, kas programmi hädaparandus mõjutas muid süsteemi elemente (näiteks andmebaasi, liidestusrakendusi, muid muudetud programmiga samasse komplekti kuuluvaid rakendusi); programmiparandust käitatakse ohjatavast programmiteegist, mida varundatakse ja säilitatakse koos lähtekoodiga mingi nõutava aja jooksul, mis põhineb muudatuse ärilisel ja õiguslikul riskil.	

Protseduur P10. Ärirakenduse muutmise ohje (jätkub)

	Kontrollida, kas IS kõrgem juhtkond vaatab õigeaegselt läbi kõik hädamuudatused ja nendega seotud juurpõhjused.	
	Hädaolukorra dokumenteerimiseks luuakse ta asetleidmisel kontrolljäljed ja logid. Kontrollida, kas hädaolukord on probleemihaldussüsteemis (näiteks konsultatsioonipunktis) täielikult dokumenteeritud, näidates ta olulist tõsidust, mis viitab vajadusele teha viivitamatult programmimuudatusi; see probleemihalduse protsess hõlmab vähemalt ühelt äritegevuse omanikult saadud auditi asitõendeid selle kohta, et on toimunud tõsine ärisüsteemi tõrge või on riknenud ärialane teave. Kontrollida, kas probleemihaldussüsteemis on tehtud märkmeid, sealhulgas hädamuudatuse või -paranduse sooritamise kuupäeva ja kellaaja kohta.	
	Programmeerijad võivad olla suutelised viima sisse hädaprogramme (see sõltub IS organisatsiooni suurusest). Kui programmeerijad ei saa kasutada elementide muutmiseks tootmiskeskkonnas oma tavalisi pääsumeetodeid, mida nad kasutavad arenduskeskkonnas, tuleb kontrollida, kas programmeerija peab juurdepääsuks tootmiskeskkonnale (näiteks programmiteegile) saama tootmistalituse, arvutikäituse või turvatalituse (st mingi rakenduste väljatöötajaist sõltumatu rühma) kontrolli all hädaolukorra kasutajatunnuse.	
	Teha kindlaks, kas hädamuudatuse ajal toimuvad tegevused logitakse ja need vaatab läbi juhtkond koos rakenduse väljatöötajate rühmaga ja turvateenuste rühmaga (näiteks suurte õigustega kasutajatunnuse tõttu, mis anti programmeerijale süsteemi käideldavust taastava hädamuudatuse tegemiseks). Asjakohase kinnituseta taaskasutuse vältimiseks peaks turvatalitus hädaolukorra kasutajatunnuse parooli tühistama.	
	Kontrollida, kas pärast süsteemi tagastamist kasutamiseks kliendile kõrvaldatakse programmeerija juurdepääs tootmiskeskkonnale (programmide ja andmete teekidele ja andmebaasidele).	
	Vaadata läbi parandusmeetmed muudatuse kordumise vältimiseks. Kontrollida, kas on vajalik ja on sooritatud täielik tõrkejärgne analüüs koos juurpõhjuse tuvastuse analüüsiga; tõrkejärgse analüüsi tulemusena on vajaduse korral rajatud uusi vältimismeetmeid (näiteks kui juurpõhjuseks osutus eelmise muudatuse adekvaatse testimise puudumine, on võib-olla vaja lisada testimise halduse meetmeid). Tavaliselt on süsteemi tõrgete ja tootmiskeskkonna muudatuste ohje protsessi nõrkuse vahel tugev korrelatsioon; on adekvaatsed ja on rangelt kasutusel need protseduurid, millega kontrollitakse, kas pärast hädamuudatust on vajalik ja on sooritatud täielik regressioontestimine, et teha kindlaks, kas programmi hädaparandus mõjutas teisi süsteemi elemente (näiteks andmebaasi, liidestusrakendusi, muid muudetud programmiga samasse komplekti kuuluvaid rakendusi).	
	Vaadata läbi hädaprogrammide käitust reguleerivad meetmed, sealhulgas kontrollida, kas programmiparandusi käitatakse ohjatavast programmiteegist, mida vaatab läbi tootmise juhtimise rühm. Kontrollida, kas tootmise juhtkond vaatab läbi kõik asjakohased süsteemi logid mõistliku kinnituse saamiseks sellele, et on tehtud ainult hädaparandusega seotud muudatusi; programmiteeke, milles asuvad hädaprogrammid (nii lähte- kui ka laadeprogrammid), varundatakse ja säilitatakse koos lähtekoodiga mingi nõutava aja jooksul, mis põhineb muudatuse ärilisel ja õiguslikul riskil; nõutakse, et kõik hädaparandused peavad tootmiskeskkonda viima arvutikäituse töötajad (seal, kus see on praktiline), mitte programmeerijad.	
	Teha kindlaks, kas alusvariandi halduse terviklus säilib, vaadates läbi alusvariandi halduse protsessi kinnituse saamiseks sellele, et programmi hädaparandused, mis jäävad püsivalt alusvariandi osaks, on sinna viidud ja välditakse hädaparanduste ja vahetult eelnenud programmimuudatuste (mis tuleb üle viia tootmiskeskkonda) ülekirjutus.	

	Kui hädamuudatuse taotluse vajaduse puhuks on kasutusel mingi formaalne protsess, kontrollida, kas on olemas kontrolljäljed, sealhulgas tüüpne muudatustaotluse vorm, mis nõuab, et muudatuse andmikus olevate plaaniväliste muudatuste kohta dokumenteeritakse ärivajadus (hädamuudatuste, plaaniväliste muudatuste ja möödumismuudatuste puhul), installeerimisplaanid ja taganemisplaanid; muudatustaotluse vormidele on kehtestatud adekvaatne säilitusperiood; järelläbivaatuse ühe osana kõrvutatakse neid muudatusi probleemiavaldusega; muudatuste registreerimise dokumentatsioon nõuab, et spetsifitseeritakse riski suurus (tõsidus), mis õigustab muudatuse tegemist standardprotsessist möödumiseks; pärast paranduse tegemist nõutakse äritegevuse omanike (asjakohasel juhtkonna tasemel) kinnitust neile parandustele.	

9 JÕUSTUMISKUUPÄEV

9.1 See protseduur kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. oktoobril 2006 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

Protseduur P11. Elektrooniline arveldus (EFT)

1 SISSEJUHATUS

1.1 Toetumine COBITile

1.1.1 Toetumine COBITile pakub spetsiifilisi COBITi eesmärke või protsesse, mida tuleks arvestada selles protseduuris käsitletava ala läbivaatusel. Konkreetse auditi käsitlusalale kohaldamiseks valitakse COBITist kõige asjakohasem materjal spetsiifiliste COBITi IT-protsesside valimise põhjal ja arvestades COBITi teabekriteeriume.

1.1.2 Elektroonilise arvelduse teostuse ja auditeerimisprotsessi jaoks on kõige asjakohasemad esmased teabekriteeriumid järgmised:

- toimivus,
- tõhusus,
- konfidentsiaalsus,
- terviklus,
- käideldavus,
- usaldatavus,
- vastavus.

1.1.3 Teostamise ja auditi sooritamisel on asjakohased järgnevaid protsesse käsitlevad COBITi juhised.

- Tehingute ja dokumentide terviklus ja turvalisus:
  - PO2 – Määratleda infoarhitektuur
  - PO9 – Kaalutleda IT riskid ja hallata neid
  - TT5 – Tagada süsteemide turvalisus
  - TT11 – Hallata andmeid
  - SH2 – Seirata ja hinnata sisejuhtimist
  - SH3 – Tagada vastavus välisnõuetele
- Tugisüsteemide toimivus ja usaldatavus:
  - HE1 – Tuvastada automatiseeritud lahendused
  - HE3 – Hankida tehnoloogia infrastruktuur ja hooldada seda
  - HE6 – Hallata muutusi
  - HE7 – Installeerida ja akrediteerida lahendused ja muudatused
  - TT1 – Määratleda teenusetasemed ja hallata neid
  - TT2 – Hallata kolmandate poolte teenuseid
  - TT3 – Hallata sooritust ja suutvust

Protseduur P11. Elektrooniline arveldus (EFT) (jätkub)

- TT4 – Tagada pidev teenus
- TT7 – Koolitada kasutajaid
- TT9 – Hallata konfiguratsiooni
- TT12 – Hallata füüsilist keskkonda
- TT13 – Hallata käitust
- SH1 – Seirata ja hinnata IT sooritust

1.2 Elektrooniline arveldus

1.2.1 Elektrooniline arveldus (EFT) on laialt kasutatav meetod arvelduskorralduste elektrooniliseks ülemaailmseks edastuseks. Need arveldused võivad olla maksekorraldused rahandusasutustele (makseteks töötajatele, ettevõtetele või üksustele) või ülekandekorraldused kliendi raha hoiustuse muutmiseks asutuses. Kliendiks võib selles kontekstis olla individuaalne tarbija või kollektiivklient.

1.2.2 EFT protsessid on üldiselt kavandatud nii, et oleks tagatud klientidele antavate EFT-teenustega seotud põhitingimuste, maksumuste ja õiguste adekvaatne avaldamine. EFT-teenuseid andvad asutused peavad klientidele avaldama teatava teabe, sealhulgas

- algsed ja ajakohastatud EFT tingimused,
- tehinguteabe,
- perioodilised tegevusteated,
- kliendi võimaliku vastutuse volitamata arvelduste eest,
- vigade lahendamise õigused ja protseduurid.

1.2.3 EFT-teenustega hõlmatakse näiteks

- rahaautomaadid,
- telefoniarvete maksmine,
- jaekaupluste kassaterminalid,
- Interneti kaudu algatatavad arveldused,
- eelnevalt volitatud ülekanded kliendi kontole või kliendi kontolt.

1.2.4 Käesoleva auditiprotseduuri otstarbeks on tehingute tüüp ja käsitlusala järgmised.

- EFT on igasugune osapoolte või hoiuasutuste vaheline rahaülekanne samal maal või eri maades asuvate elektrooniliste andmesüsteemide kaudu. EFT võib toimuda sama hoidja või eri hoidjate (pankadevahelise, ettevõtetevahelise tehingu) kontode vahel.
- EFT ei eelda küll e-kaubandust, kuid seda võib vaadelda ettevõtetevahelise mudeli (B2B) rakendusena.

- Kõiki muid e-kaubanduse mudeleid (ettevõtte ja kliendi (B2C), kliendi ja ettevõtte (C2B) vahelise jt), mis üldiselt sisaldavad kaarditehinguid, loetakse kassahaldustehinguteks.
- Kogu käesolevas dokumendis hõlmab termin ka pankasid ja muid selletaolisi asutusi, kus on kasutusel EFT.

1.2.5 Sõltuvalt konkreetsest rakendusest võivad tehingu allikad olla järgmised.

- Rahaautomaat (ATM). Klient sooritab sisemaise tehingu pangaga, mis on seotud ATM-võrguga. Kasutatakse sihtkliendi kontot.
- Elektroonilise ülekande korraldused ja võrgupanganduse rakendused pangalt, mis annab selle võimaluse oma veebiteenuste osana.
- Pangalett, kus klient täidab ülekande kviitungi teisele sise- või välismaisele pangale.
- Panga rahandusabi talitus või klienditeenindus, kus klient annab panga töötajale korralduse sooritada elektrooniline tehing teise pangaga.
- Automatiseeritud arvelduskodade (ACH) võrk. See on pakktöötluslik elektroonilise arvelduse süsteem, mis tagab osalevatele rahandusasutustele pankadevahelise elektrooniliste maksete arvelduse.
- Kassaterminal, mis võimaldab jaemüüjal hallata raha, kaubavaru ja kliente.
- Ettevõtte ressursside plaanimise süsteem (ERP) või selletaoline rakendus, milles ettevõte genereerib EFT-faili, mis edastatakse pangasüsteemile.
- Teleksi- või faksitehing võtmete raamatuga.

1.2.6 Kõigi jaotises 1.2.4 loetletud teostuste puhul on süsteemis mingi eesteenus või –rakendus, mis haldab kliendiliidest, genereerib korralduse ja saadab selle tagarakendusele (tuumrakendusele), mida haldab pank globaalse tehinguvõrgu (näiteks SWIFT, MERVA, FED Wire) kaudu.

1.3 Rakenduste või tehnoloogiaplatvormide tüüp

1.3.1 Eesrakenduse tehnoloogia sõltub ettevõtte rakendusest (ERP liidestest) ja panga teenustest (ATM-id, konsultatsioonipunkt, letitehingud, võrgupangandus).

1.3.2 Rakendused, platvormid või vahetarkvara võivad põhineda klient-server-arhitektuuril (LAN/WAN, st ERP-d), pärandrakendustel (kõik platvormid), veebirakendustel (Internet) või spetsiifilistel rakendustel (ATM-võrgud).

1.3.3 Taga- ehk tuumrakendus on EFT protsessis väga oluline komponent, sest just see rakendus kannab lõplikult raha üle ühelt kontolt teisele, ühest pangast teise ja üldjuhul ühest riigist teise. Seetõttu pangad üldiselt ei võimalda veebitehnoloogia platvormi teostusi, vaid kasutavad usaldusväärsema tehnoloogia platvormi teostusi, mis põhinevad suurarvutil (näiteks IBM OS400), millel on andmebaas operatsioonisüsteemi sisse ehitatud, nii et saadakse suurem turvalisus ja jõudlus.

Protseduur P11. Elektrooniline arveldus (EFT) (jätkub)

2 EFT PROTSESS

2.1 Määratlus

2.1.1 EFT on raha elektrooniline ülekandmine ühelt kontolt teisele ühes ja samas ettevõttes või ühest ettevõttest teise.

2.1.2 EFT on keeruline protsess, kus ülekandeid võidakse sooritada mitmesuguste meetoditega ja mitmesuguses vääringus. EFT nõuab väga tõhusate turvameetmete sisseehitamist süsteemidesse ning protsessi ohjatakse nii saatja kui ka vastuvõtja poolel. Vahejärkudes peavad turvameetmed olema kõikjal, kus teavet edastatakse, talletatakse või töödeldakse.

3 RISKI HINDAMINE JA TURVAMEETMED

3.1 Riskid. IT üldmeetmed

3.1.1 Üldiselt peaks EFT protsess tagama konfidentsiaalsuse, tervikluse ja käideldavuse (CIA). Teostuse eritüübi puhul võib aga prioriteedijärjestus olla CIA asemel IAC (terviklus, käideldavus ja konfidentsiaalsus). See nõue tuleks täita turvameetmetega, mida rakendatakse EFT teostuse eri tasemetel, näiteks äriprotsessi meetmetega, rakenduse meetmetega ja platvormi meetmetega.

3.2 Äriprotsessi meetmed

3.2.1 Üldiselt tuleks äriprotsessidel tagada EFT protsesside CIA.

3.2.2 Ükski isik ei tohiks käsitleda kogu tehingut. Selle nõude täitmiseks tuleb õigesti lahutada tegija ning kontrollija ja saatja kohustused.

3.2.3 Tehingukorralduste terviklus ja õigsus tuleks säilitada allikast sihtkohani. Asjakohane ohje peaks hõlmama kontode kooskõlastamist, asjakohaste kontode ning tehingu genereerimise kuupäeva ja kellaja kontrollimist, kontode ja tehingute üksikasjadele kinnituse saamist klientidelt jne. Faksitehingute puhul võetakse vaatluse alla eelkõige

- võtmeraamatu protseduurid,
- autentimisnõuded,
- võtme genereerimine,
- võtme hoidmine, vahetus ja tühistamine,
- võtmeprotseduuridest teavitamine.

3.2.4 Tehing tuleks taotleda, genereerida ja sooritada vastavalt kokkulepitud teenusetasemelepetele (SLA).

3.2.5 SLA kliendinõuete täitmise tagamiseks tuleks asjassepuutuv personal adekvaatselt koolitada.

3.2.6 Rahandusasutusel peaks olema mõistlik palkamiseelse taustakontrolli protsess ja peaksid olema piisavalt katvad konfidentsiaalsuslepped.

3.2.7 Tuleks arvestada töötajate sidumist sisemise pettuse peletamise eeskirjadega.

3.2.8 Tuleks arvestada saate ja vastuvõtu poole riikide õigusnormide mõju ning tuleks tagada vastavus kõigile piire ületavaid tehinguid puudutavatele nõuetele.

3.2.9 Süsteemi või võrgu väljalangemise puhuks peaksid olema jätkusuutlikkuse protseduurid ja EFT tehingute edastuse alternatiivsed viisid.

3.2.10 Äriprotsessi meetmete hulka kuulub sobivate andmete kogumine soorituse mõõtmiseks võrreldes kokkulepitud SLA-ga. Ideaaljuhul tuleks EFT mõõdustikku arvutada ja analüüsida kõigi EFT tehingute protsesside kohta. Mõõdustiku analüüsimisel tuleks arvestada lepingute mõju ja SLA määratlusi.

3.3 Rakenduste meetmed

3.3.1 Rakendustaseme meetmed peaksid tagama edastuskorralduste konfidentsiaalsuse, tervikluse ja käideldavuse (CIA).

3.3.2 Identifitseerimise ja autentimise puhul tuleks võtta arvesse

- sisselogimine konkreetsetesse EFT terminalidesse (kitsendused terminalidele),
- staatilised või dünaamilised paroolid (parooli tugevus),
- digitaalsertifikaadid ja seansi kestuse piirangud.

3.3.3 Pääsu reguleerimise ja volituste andmise ja kinnitamise (õiguste läbivaatamise) sammud peaksid olema dokumenteeritud ja neid tuleks seirata.

3.3.4 EFT tehingute üksikasjade muudatused tuleks teha rakendusest, mis algatas tehingu. Kõiki muul viisil alguse saanud muudatusi tuleks nende võimaldamiseks asjakohaselt reguleerida sobiva identifitseerimise, autentimise ja volitamisega.

3.3.5 EFT rakenduse individuaalkasutajaile tuleks seada realistlikud tehingute maksimaalarvu ja igapäevase kogusumma piirangud. Kollektiivklientide piirangud sõltuvad SLA-st ja vastavast kliendipoliitikast.

3.3.6 Lisaks prinditavale kviitungile tuleks iga tehingut ta kinnitamiseks või ta kasutaja tähelepanu juhtimiseks kviteerida meiliga või mobiiltelefonile saadetava SMS-skriptiga.

3.3.7 Rakenduse tasemel peaksid olema sobivad muudatuste reguleerimise meetmed.

3.4 Platvormi meetmed

3.4.1 Tuleks võtta arvesse järgmised meetmed ja aspektid:

- krüpteerimine,
- algoritmi tugevus,
- võtme tugevus,

- võtmehaldus,
- suhtlus,
- krüpteerimise tüüp,
- teostus riistvaras või tarkvaras,
- ISO mudeli kiht, milles rakendatakse krüpteerimist.

3.4.2 Tuleks arvestada tehingute salgamise vääramist, näiteks digitaalsignatuuridega.

3.4.3 Andmete asukoht peab järgima eeskirju piiri ületavate tehingute kohta.

3.4.4 Side puhul tuleks võtta arvesse järgmised aspektid:

- partnerliinid või avalik võrk,
- sideprotokollid,
- krüpteerimisprotokollid,
- side erijooned, eriti kaugside puhul.

3.4.5 Tuleks võtta arvesse terviklusmeetmed, näiteks tsükliline liiaskoodkontroll (CRC), räsifunktsioon ja võtmealgoritm.

3.4.6 Tuleks kasutada riistvara, mis tagab käideldavuse ja täpsuse, suure jõudluse ja koormustaluvuse (multitegum- ja multiseansstöö).

3.4.7 Tuleks arvestada muudatuste halduse meetmeid riistvara, tarkvara ja platvormi tasemel.

3.4.8 Administreerimisfunktsioonid, mis sisaldavad muudatusi turbes ning administraatori- ja kasutajakontode parameetrite muutmist, peaksid nõudma lisavolitamist.

3.5 Pettuste avastamise ja vältimise meetmed

3.5.1 Kogu maailmas on EFT süsteemide tehingud avatud suurele riskile ja pettusetoimingutele. Keskne pettuste taga olev motiveering on rahaline kasu, vähem aga soov valitseda EFT protsessi, teo põnevus, vaimne jõuproov ja töötaja kättemaks. Suurte maksete saamiseks vajalike elementaarses tekstifailis tehtavate muudatuste lihtsus on üks pettuse sooritamisele tõukavaid tegureid. EFT pettusliku muutmisega võib isik varastada suuri rahasummasid. Statistika näitab, et avalikud ettevõtted kaotavad pettuslike EFT-maksekorralduste tõttu igal aastal tohutuid summasid.

3.5.2 Andmete iga volitamatu muutmine (pettus) või isegi andmesisestuse viga tekitab (kui seda viivitamatult ei avastata ega parandata) muudatuse kliendi kontoseisus, seetõttu on nendes süsteemides äärmiselt tähtis vältida lubamatuid muudatusi.

3.5.3 Üldiselt on eri kliente, panku ja riike hõlmavate rahaülekannete puhul väga oluline, et protsess tagaks (preventiivsete meetmetega) tehinguandmete valideerimise enne nende töötlust.

Protseduur P11. Elektrooniline arveldus (EFT) (jätkub)

3.6 EFT auditeerimise protseduur

3.6.1 Järgnev tabel on soovitatav auditeerimisprotsess, millega vaadata läbi EFT protsess (sisemised rakendused, näiteks ERP-d ja rahandusasutuste pakutav võrgupangandus).

Nõuded	Soovitatavad EFT auditi protseduurid
Üldmeetmed	Määratleda läbivaatuse eesmärk ja käsitlusala ning hankida dokumentatsioon. Hankida EFT osakonna töötajate hetkenimistu. Hankida käitatavate EFT süsteemide kirjeldus, sh rahaautomaatide, kassaterminalide, deebet-, krediit- ja kiipkaartide, võrgupanganduse, võrgus ja kaubanduses osalemise kohta. Hankida täielikud EFT protsessiga seotud üksikasjalikud protsessi ja meetmete kirjeldused. Hankida EFT protsessiga seotud poliitikad ja standardid, sealhulgas - EFT äriprotsessi puhul asjakohased infoturbenõuded, - toodetes ja rakendustes olevate kontrolljälgede käsitluse protseduurid. Hankida kõik EFT protsessile kohaldatavad õigusaktid. Hankida EFT protsessi toetamiseks kasutatava riistvara, tarkvara ja sideprotokollide täielik loetelu ja valida läbivaatuseks EFT komponendid. Riski kaalutlemiste, olemasolevate turvameetmete ja eelmiste läbivaatuste põhjal määratleda auditi käsitlusala ja strateegia. Läbi vaadata eelmise auditi aruanne ja leiud ning selgitada välja meetmed, mida juhtkond peab rakendama. Läbi vaadata andmike säilitamise poliitika ja otsustada selle adekvaatsus. Läbi vaadata ATM-alase vastutuse, tegevuse katkestuse ja usaldatavuse kate kindlustusega. Selgitada välja, kas terminalid on kindlustatud varguse, sissemurdmise ja muude ohtude eest. Selgitada välja, kas kasutajate koolitusmaterjal on dokumenteeritult olemas ja kasutamiskohal nähtaval. Selgitada välja, kas on olemas jätkusuutlikkuse ja avariihalduse plaanid.

Protseduur P11. Elektrooniline arveldus (EFT) (jätkub)

Füüsilised meetmed	Selgitada välja, kas terminalid (näiteks rahaautomaadid, kassaterminalid) asuvad turvalisel territooriumil. Selgitada välja, kas terminalid on turvaliselt lukustatud ja kas neil on installeeritud pääsu reguleerimise mehhanismid. Selgitada välja, kas terminalidele on juurdepääs ainult volitatuil. Selgitada välja, kas on olemas territooriumil suvalisel hetkel viibivate isikute maksimaalarvu piirang. Selgitada välja, kas järjekorras seisjail on võimatu vaadata ekraanil olevat kasutaja teavet. Selgitada välja, kas on olemas terminali adekvaatne juhtkonnapoolne järelevalve. Selgitada välja, milline on tellimuste vastuvõtu ruumi või tööala ümbritseva füüsilise turbe tase. Selgitada välja, kas süsteem kasutab pääsu reguleerimiseks füüsilisi pääsmikke (magnetkaarti, kiipkaarti vms). Kui jah, siis kontrollida, kas füüsiliste pääsmike vastuvõtule, hoidmisele ja väljaandmisele rakendatakse rahuldavad turvameetmed. Selgitada välja, kas on olemas mingi süsteem kasutaja kujutise ja vastavate toimingu üksikasjade hõiveks, talletuseks ja võtuks. Selgitada välja, kas sularaha paigutamine rahaautomaatidesse ja teisaldus kassaterminalidest on adekvaatselt turvatud ja kaitstud. Selgitada välja, kas terminalid on välismaailmale nähtavad või varjatud. Mõlemal variandil on oma eelised ja puudused ning mõlemal juhul tuleks rakendada korvavaid meetmeid. [10]
Protsessi-meetmed	Selgitada välja, kas EFT-ga seotud pearaamatukontosid viiakse õigeaegselt kooskõlla. Selgitada välja, kas kooskõlastuse erandid vaadatakse regulaarselt läbi ja rakendatakse vastavaid meetmeid. Selgitada välja, kas EFT süsteemi ja algatuskoha kooskõlastust ohjatakse ja vaadatakse läbi adekvaatselt. Kontrollida, kas igapäevane arveldus iga ühiskasutusliku EFT-võrguga on ajakohane ja ohjatud. Selgitada välja, kas on olemas protseduurid tehingute kooskõllaviimiseks ja kas need on ajakohased. Läbi vaadata kõik käitusprotsessi käsioperatsioonide vahendid (teleks, võtmeraamat vms). Läbi vaadata kooskõlastamise ja salgamise vääramise protseduuride toimivus. Tuvastada olemuslikud IT riskid ja kontrollpunktide üldine tase EFT protsessis. Analüüsida logide talletuse ja halduse ressursside (näiteks: võrgus, autonoomselt, samas asukohas, muus asukohas) turvet. Läbi vaadata kontrolljäljed, vastavalt vajadusele toimingu taastamiseks või vea analüüsimiseks. Läbi vaadata seadmetes või tarkvaras seatud parameetrid, mis on seotud aktiveerimise, desaktiveerimise või kustutusega. Hankida riski kaalutlemise dokumendid iga genereeritava konrolljälje kohta ja hinnata neid.

[10] Varjatud terminalid pakuvad küll kasutajale privaatsust, kuid ühtlasi annavad nad varju ka sissetungijale või kelmuse sooritajale. Nähtavad terminalid ei anna varju kelmuse sooritajaile, kuid nende puuduseks on see, et kõrvalised saavad jälgida terminali juures toimuvat.

Protseduur P11. Elektrooniline arveldus (EFT) (jätkub)

Protsessi-meetmed (jätkub)	Kontrollida, kas EFT kontrolljälgedele on rakendatud turvameetmed (näiteks seadmetes, võrgus, protseduurides). Seirata rutiine kontrolljälgede olemasolu analüüsimiseks. Läbi vaadata turvatarkvara või võtmehalduse aruannete kontrolljäljed. Läbi vaadata side turvameetmed (krüpteerimise, autentimise) CIA tagamiseks ja hinnata neid. Hinnata elutähtsate andmete ja dokumentide talletust ning logide säilitamist. Hinnata vastavust sisemistele ja regulatiivsetele nõuetele. Hinnata väljasttellimisteenuseid (kui neid on). Läbi vaadata ERP-s genereeritava EFT-tekstifaili pääsutase. Läbi vaadata EFT klienditarkvara muutmispääsu tase. Läbi vaadata EFT klienditarkvara turbe, halduse ja kasutajakonto parameetrite turvameetmed.
Edastuse ja süsteemi tõrked	Selgitada välja, kas süsteem edastuse katkemisel registreerib aktsepteeritud sõnumid. Selgitada välja, kas aktsepteerimata sõnumite kordamiseks on olemas kirjalikud protseduurid Selgitada välja, kas kõigi normaalse töötlusekatkestuste kohta peetakse intsidentide logi. Selgitada välja, kas riistvara tõrke puhul saab töötluse ümber lülitada teisele terminalile. Selgitada välja, kas on olemas meetmed sõnumi töötluse kordamise vältimiseks pärast süsteemi taastumist. Selgitada välja, kas liini rikke puhuks on olemas varu-sidekanal.
Süsteemi sisselogimise turvameetmed	Selgitada välja, kas süsteem valideerib kõiki volitatud kasutajaid. Selgitada välja, kas seansiteed saavad luua ainult volitatud isikud. Selgitada välja, kas süsteem registreerib seansitee looja või sisselogija. Selgitada välja, kas süsteem registreerib kõik katsed töötada väljaspool lubatavaid funktsioone. Kui see on nii, teha kindlaks, kas neid andmeid vaadatakse perioodiliselt läbi ja rakendatakse asjakohaseid meetmeid. Selgitada välja, kas süsteem registreerib kõik parooli kasutamise või sisselogimise rikkumised ja kas neid andmeid vaadatakse regulaarselt läbi. Selgitada välja, kas süsteem seansi loomisel valideerib terminali identifikaatorit. Selgitada välja, kas süsteem nõuab kliendi kui volitatud kasutaja valideerimiseks turvalise võtme kasutamist. Selgitada välja, kas süsteem kontrollib enne edastust kõigi sõnumite lubatavust. Selgitada välja, kas süsteem väldib lubamatute sõnumite edastuse. Selgitada välja, kas süsteem kontrollib kasutaja volitatust kõnealust tüüpi sõnumi saatmiseks. Selgitada välja, kas on olemas protseduurid lubamatutest sõnumitest teatamiseks edastuse ajal. Selgitada välja, kas kontrollitakse kõigi sisenddokumentide asjakohast allikapoolset volitamist. Selgitada välja, kas on olemas meetmed, millega tagada, et sõnumite igapäevane või isikukohane väärtusepiirang on asjakohaselt volitatud.

Protseduur P11. Elektrooniline arveldus (EFT) (jätkub)

Sõnumi-vahetuse meetmed	Selgitada välja, kas igale sõnumile kinnistatakse järjenumber katkematust jadast. Kui see on nii, kontrollida, kas nad on jäädvustatud sisenddokumentides või -registris. Selgitada välja, kas katkestused vaadatakse läbi. Selgitada välja, kas kõigi edastatavate sõnumite kohta peetakse püsivat andmikku. Kui see on nii, kontrollida, kas seda võrreldakse kõigi aktsepteeritud või ärajäetud sõnumite andmikuga. Selgitada välja, kas on võimalik võtta individuaalsõnumi andmeid. Selgitada välja, kas kõigi sisendsõnumite kohta luuakse kontrolljälg ning kas selles jäädvustatakse - sõnumi ühene viitenumber, - sisestuse kuupäev ja kellaaeg, - sisestuse kontrollija või volitaja, - seansitee looja, - edastuse kuupäev ja kellaaeg, - sõnumi aktsepteerimine või sellest keeldumine, - sõnumi sisu üksikasjad. Selgitada välja, kas revisjonilogi väljastatakse kellelegi sõltumatult sisestusfunktsioonist. Selgitada välja, kas revisjonilogidele on juurdepääs ainult selleks volitatuil. Selgitada välja, kas juhtkond uurib revisjonilogisid. Selgitada välja, kas saadetavaid sõnumeid ja kontokokkuvõtteid kooskõlastatakse omavahel regulaarselt. Selgitada välja, kas kõigile sõnumiallikatele teatatakse nende saadetud sisendsõnumite aktsepteerimisest.
Ülekande meetmed	Sisenevate ülekannete meetmete puhul selgitada välja, kas - kõik sõnumid saadetakse standardvorminguga, - standardvormingute muutmine on keelatud, - süsteem tagab kõigi valideeritud väljade sisestuse, - süsteem tagab kõigi väljade sisestuse nõutavas vormingus, - süsteem teatab oodatavast vahemikust väljuvatest summadest või tõstab need esile, - on olemas meetmed, millega tagada, et ei aktsepteerita väärtusi, mis väljuvad eeldatavaist piiridest, - on olemas meetmed, millega tagada, et sõnumite koguväärtus on kokkulepitud (päeva)piirides; - süsteem kviteerib ülekantud sõnumite rahuldavat valideerimist. Väljuvate ülekannete meetmete puhul selgitada välja, kas - sõnumi sisestamine toimub teda ümber kirjutades, - volitav ametnik võrdleb kõiki sõnumeid allikdokumentidega, - allikdokumendid on sisestamise ja volitamise ajaks asjakohaselt kinnitatud, - süsteem sunnib lahknevuste korral uuesti sisestama ja nõuab tõestust, - vaadatakse läbi kirjalikke protseduure vigade käsitluseks, - süsteem genereerib sisestatud sõnumite arvu ja väärtuse kontrollsummad ja võrdleb neid sisendandmikega, - süsteem koostab aruande kõigi aktsepteeritud ja tagasilükatud sõnumite kohta, koos kontrollsummadega ja võrdleb neid sisendandmikega, - tagasilükatud sõnumite käsitluseks on olemas kirjalikud protseduurid, - süsteem genereerib mingeid kontrollsummasid vms, - sideprotokoll kasutab veaavastuse ja veaparanduse meetodeid.

Protseduur P11. Elektrooniline arveldus (EFT) (jätkub)

PIN-koodi meetmed	Läbi vaadata PIN-koodi väljaandmise protseduur. Selgitada välja, kas PIN-koodid on säilituse ja edastuse ajal adekvaatselt kaitstud. Läbi vaadata PIN-koodi salvestuse krüpteerimise protseduurid. Läbi vaadata PIN-koodide väljastusturbe protseduur. PIN-koodid peavad olema väljastamisel varjatud ega tohi olla trükitud kujul, kergesti nähtavad või seostatavad kliendi kontonumbritega. Koodide eest vastutaval personalil ei tohi olla võimalik näha ega süsteemist saada kliendi PIN-koodi. Selgitada välja, kas PIN-kood postitatakse kliendi kaardist lahus. Kõige soovitatavam abinõu on saata PIN-kood ja kaart lahus kahe eri teenuseandja kaudu. Selgitada välja, kas PIN-koodi süsteem takistab juurdepääsu kliendi kontole pärast mingit väikest arvu nurjunud katseid. Läbi vaadata nurjunud sisselogimiskatsed ja kliendi või organisatsiooni rakendatud meetmed. Läbi vaadata unustatud PIN-koodide käsitluse ja uute väljaandmise protsess.
Kaardi turvameetmed	Läbi vaadata kaardi väljaandmise protseduur, sealhulgas - kaartide soetamise protseduuri ohje adekvaatsus, - kirjalik kokkulepe kaarditootjaga, - kaarditootja auditiaruanne, - kaartide klientidele postitamise ja kohaletoimetuse turvameetmed. Selgitada välja, kas kaardid postitatakse koos saatja aadressiga (juhuks, kui ei jõua adressaadini) ja lahus PIN-koodide saatmisest. - tagasisaadetud kaartide ja kaotatud kaartide käsitluse protsess, - kinnipeetud või kogemata EFT-terminali jäetud kaartide käsitluse protsess, - test- või demokaartide ohje, - võimaliku kiirkaartide süsteemi turvameetmed. Läbi vaadata kaardi kasutamine: - kaardi aktiveerimine, - väljaantud ja aktiveerimata kaardid, - kliendi andmete ja kontoga seotud teave, - suletud kontod, soikunud kontod, surnud kontod. Läbi vaadata leping kaarditootjaga, kaarditootja kvaliteediprotsess, meetmed, mis ei võimalda kaarditootjal ega ta töötajail genereerida volitamata kaarte, ning adekvaatse kaitse olemasolu tootja tegevuse lõppemise puhuks.
Pettuse vältimine	EFT-ga seotud pettuse vältimise mehhanismi olemasolus veendumiseks vaadata läbi - EFT protsess ja kontrollpunktid, - EFT poliitikad ja protseduurid, - standardsed ülekannete vormingud, - kõiki EFT komponente ümbritsev füüsiline turve, - EFT rakenduse turbe toimivus, - võrguoperatsioonisüsteemi toimivus, - EFT andmeid ümbritseva füüsilise turbe toimivus, - süsteemi logimise toimivus, - (tegija, kontrollija ja saatja) kohustuste lahususe toimivus, - kontode kooskõlastused, - haldusfunktsioonide kaasvolitamine EFT rakenduse maksimaalse tehingumahu ja päevase kogumahu piires, - kasutamismustrite (näiteks sisselogimiste sageduse, raha väljavõtmiste, samal päeval toimunud väljavõtmiste, kasutamistundide arvu) jälitus võimaliku rahapesu või petmiskavatsuse avastamiseks.

Protseduur P11. Elektrooniline arveldus (EFT) (jätkub)

Tagarakendus	Tagarakendused on üldiselt platvormispetsiifilised. Selgitada välja, kas tagarakendustega tagatakse - atomaarsus: tööüksust ei tükeldata, kõik toimingud õnnestuvad või nurjuvad; - kooskõla: kui tehing ei saa genereerida üht stabiilset olekut, peab ta naasma oma algolekusse, - isolatsioon: ühe tehingu käitumine ei saa mõjutada teisi samal hetkel sooritatavaid tehinguid, - püsivus: tehingu toimed on püsivad, neid ei saa mõjutada süsteemi tõrked.
Eesrakenduse ja perimeetri turve	Kui eesrakendused on veebipõhised, vaadata läbi avatus lisariskidele, mida võivad tekitada näiteks - teenusetõkestus, - viirused, nuhkimine ja andmete väljapetmine teesklusega, - turvaaukude paikamise protseduuride puudumine; - veebiserveri turvaaugud, - väär arhitektuur ja konfiguratsioon (tulemüürid, sissetungi tuvastuse süsteemid, DMZ). ATM-eesrakenduste puhul arvestada PIN-koodide nõrkust, ebapiisavat teadlikkust, krüpteerimise puudumist jms.
Tehingupäevik	Selgitada välja, kas tehingupäeviku teabes on järgmised andmed: - sisenev päringutehing, - sisenev ajakohastustehing, - tehingu tüüp, - tehingu number, - valuuta, - valuuta kurss, - summa, - kontonumbrid, - panga marsruutimisandmed, - allikterminal, - allikoperaator, - kellaaeg ja kuupäev, - päringuvastuse tehing, - ajakohastusvastuse tehing, - vastuse õige vastuvõtu tunnus, - protseduuri rikkumine sisestamisel, - faili rekonstrueerimise alguse ja lõpu kirje, - ajakohastuse lõpu teade. Võtta arvesse ka - päevikutehingute säilitus, - säilitamine ja varundus, - õigusaktide ja põhikirja nõuded.

Protseduur P11. Elektrooniline arveldus (EFT) (jätkub)

Kontrolljäljed	Selgitada välja, kas süsteemil on päevikud ja logid. Selgitada välja, kas kontrolljälg võimaldab - audiitoril jälgida tehingu ajalugu, - taastada kirjet, kui ilmneb, et kasutaja on selle vääralt uuendanud või kustutanud, - uurida vigaste kirjete ilmnemise juhtumeid, - aidata taastada faile pärast nende massiivset hävimist, - aidata parandada faili, kus programm kahjustas andmeid, - võimaldab parandada süsteemi kasutajaile saadetud väära teavet, - seirata protseduuride rikkumisi võimalike turvalisuse rikkumiste esiletoomiseks, - aidata süsteemi õigesti taastada pärast ta väljalangemist, - seirata süsteemi kasutamise viisi, - taastada teavet pärast muude päevikulogide hävimist, - olla kooskõlastusaruannete allikaks, - arvestada säilitamise ajal regulatiivseid nõudeid ja teenuste eesmärke.

4 JÕUSTUMISKUUPÄEV

4.1 See protseduur kehtib kõigi infosüsteemiauditite kohta, mis algavad 1. mail 2007 või pärast seda. Täieliku ingliskeelsete terminite sõnastiku võib leida ISACA veebisaidist aadressil *www.isaca.org/glossary*.

LISA

Allikaviited

ISACA. Infosüsteemide juhtimise ajakiri. USA. November 1999, jaanuar 2000, september 2002, juuli 2003.

IT Halduse Instituut. COBIT 4.0. USA. 2005.

Peltier, Thomas R. Infosüsteemide riskianalüüs. Auerbach, USA. 2001.

Infosüsteemide juhtimise spetsialistide standardid

Välja andnud Infosüsteemide auditi ja juhtimise assotsiatsioon (ISACA)

510. Käsitlusala sõnastus

510.010 Vastutus, volitused ja aruandluskohuslus

Asjakohane juhtkonna aste peab asjakohaselt dokumenteerima ja heaks kiitma infosüsteemide (IS) juhtimistalituse vastutuse, volitused ja aruandluskohusluse.

520 Ametialane sõltumatus

520.010 Ametialane sõltumatus

Kõikides IS juhtimisse puutuvates asjaoludes peab IS juhtimise spetsialist säilitama sõltumatu hoiaku ja esinemisviisi.

520.020 Organisatsioonilised suhted

IS juhtimise talitus peab olema kontrollitavast valdkonnast piisavalt sõltumatu, et IS juhtimise spetsialist saaks oma töökohustusi erapooletult täita.

530. Kutse-eetika ja ametialased standardid

530.010 Kutse-eetika koodeks

IS juhtimise spetsialist peab kinni pidama "Infosüsteemide juhtimise spetsialistide kutse-eetika koodeksist", mille on välja andnud Infosüsteemide auditi ja juhtimise assotsiatsioon (ISACA).

530.020 Nõuetekohane tööalane hoolsus

Kõikides IS juhtimise spetsialisti tööala aspektides peab rakendama nõuetekohast tööalast hoolsust ning järgima kohaldatavaid erialastandardeid.

540. Pädevus

540.010 Oskused ja teadmised

IS juhtimise spetsialist peab olema tehniliselt pädev ning valdama oskusi ja teadmisi, mis on vajalikud juhtimise spetsialisti töö sooritamiseks.

540.020 Pidev erialane enesetäiendus

IS juhtimise spetsialist peab säilitama pädevuse, toetudes asjakohasele erialasele täiendõppele.

550. Plaanimine

550.010 Juhtimise plaanimine

IS juhtimise spetsialist peab juhtimiseesmärkide käsitlemiseks kasutama riskikaalutlemis- ja muid tööriistu, mis on asjakohased IS juhtimistöö plaanimisel ja prioritiseerimisel.

Infosüsteemide juhtimise spetsialistide standardid (jätkub)

560. Töö sooritamine

560.010 Järelevalve

IS juhtimise spetsialistidele tuleb rakendada asjakohane järelevalve ja neid koordineerida kinnituse saamiseks sellele, et juhtimise esmärgid saavutatakse ning kohaldatavaid kutsealaseid standardeid järgitakse.

560.020 Tõendusmaterjalid

IS juhtimise spetsialist peab säilitama piisavad, usaldusväärsed, asjakohased ja kasulikud tõendusmaterjalid tegevuste ja ülesannete kohta, mis on sooritatud juhtimiseesmärkide saavutamiseks. Juhtimise hindamist peab toetama tõendusmaterjali asjakohane analüüs ja tõlgendamine.

560.030 Mõjusus

IS juhtimise spetsialistid peavad oma töökohustuste täitmisel rajama asjakohased mõõdupuud oma tegevuste mõjususele, et saavutada nii oma rolli eesmärgid kui ka eesmärgid, mis on määratletud "Käsitlusala sõnastuses".

570. Aruandlus

570.010 Korraline aruandlus

IS juhtimise spetsialist peab asjakohasele juhtkonna astmele regulaarselt aru andma, mis ulatuses on juhtimiseesmärgid saavutatud.

580. Järeltoimingud

580.010 Uus läbivaatus

IS juhtimise spetsialist peab seirama juhtimisprotseduuride sooritust, läbi vaatama tagasisidet juhtimistegevuste tõhususe ja toimivuse kohta ning tagama, et vajalikes kohtades rakendatakse asjakohased parandusmeetmed.

Jõustumiskuupäev

See teave anti välja 1. mail 1999 ja kehtib kõikidele IS juhtimistegevustele, mis algavad või toimuvad pärast 1. septembrit 1999.