How to build a resilient business?

ISACA Estonia

—

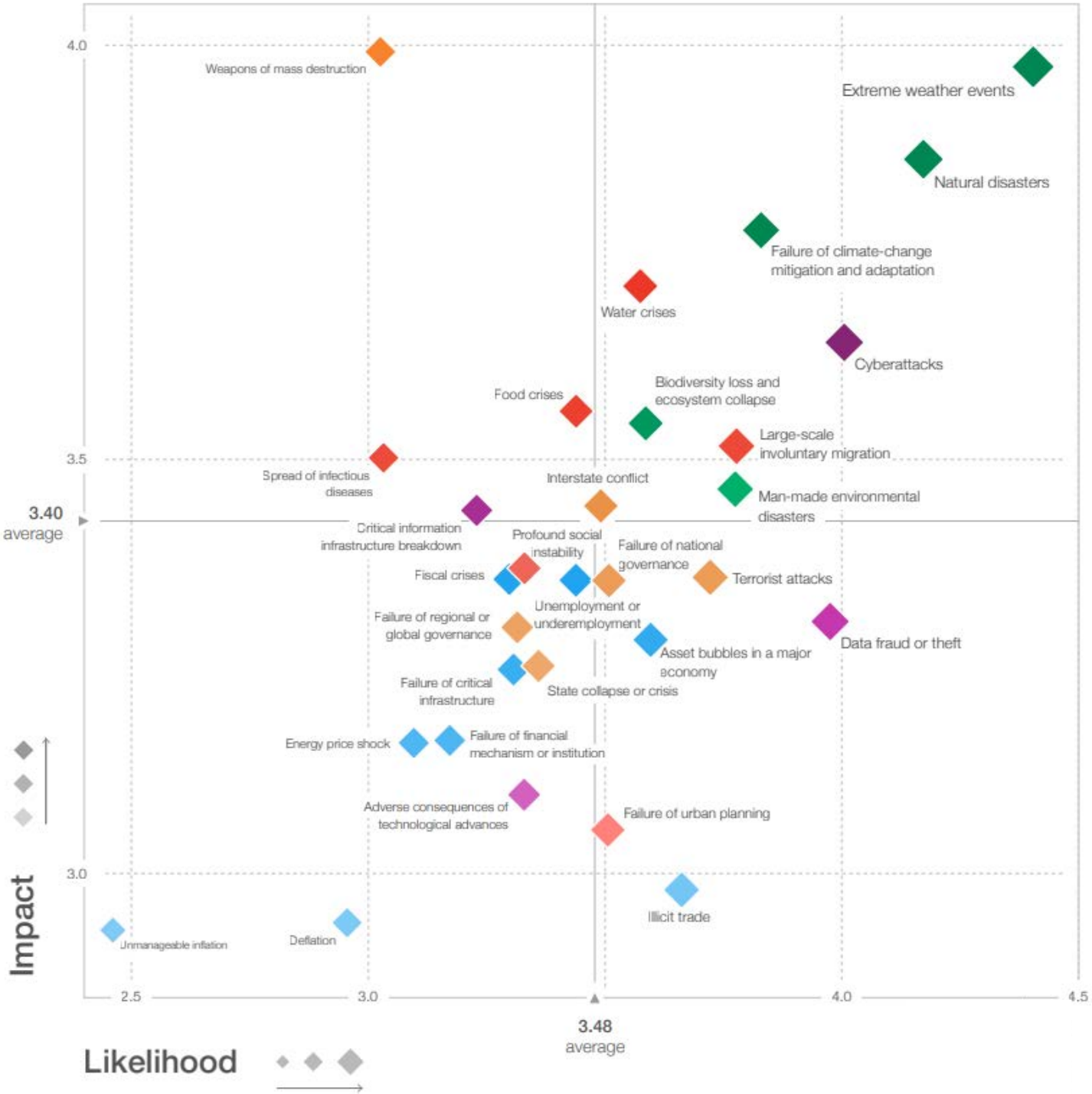
January 2019

Topics for the day

- Requirements for business continuity
- Building blocks for business continuity management
- Top 10 incident response mistakes
- ISO 22301 certification – Case Telia

KPMG

Brief view on risk landscapes



WORLD ECONOMIC FORUM

The Global Risks Landscape 2018

http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Technology based business risk management

Technology provides many benefits, at the same time, it introduces major risks on several crucial fronts that need to be governed and managed by user organizations.

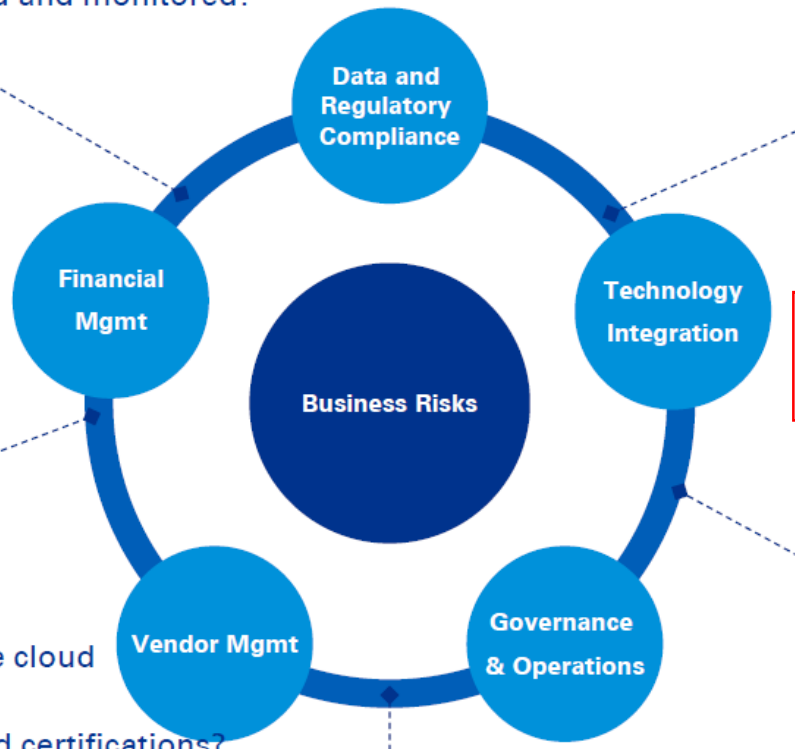
Well-managed organizations must understand and mitigate these risks to better leverage their e.g. cloud computing initiatives. Five major risks areas are:

1. **Data security and regulatory**
2. **Technology**
3. **Operational**
4. **Vendor**
5. **Financial**

Source: KPMG 2016, Moving to the cloud – key risk considerations

KPMG

Data driven risks for Cloud



- Do I know where my data is located in the cloud?
- Has data been classified as per company policies and secured accordingly?
- Am I aware of the compliance requirements to be met?
- Is member data appropriately isolated, segregated and masked?
- What accounts do I have in the cloud and is access to confidential data logged and monitored?

- How do I account for spending in the cloud and by who?
- What is my financial exposure?
- Is there a consistent approach to defining the business case for leveraging cloud solutions?
- Is there a clear process to predict and manage spending on cloud solutions?

- Have I integrated the cloud environment to leverage existing IT and technology services?
- Are my production and development environment appropriately segregated?
- Do I have a process to monitor for evolving technology?

- Is there a clear process to manage cloud procurement?
- Does the vendor have the required certifications?
- How stable is the provider?
- Have expected contract terms and conditions, including SLA, been defined for cloud vendors?
- Is there monitoring of cloud vendors to ensure they meet compliance requirements and controls?
- Is there a defined exit strategy?

- Is the cloud strategy operationalized across the organization through a governance model and exception management?
- Is my cloud application backed up appropriately?
- Is there DR in place?
- Do I have a process to monitor SLA compliance?

Where is the buzz?

Buzz Top 3

Most popular trends

▲ 1%	Digital Payments
▼ -5%	Robotics
▲ 6%	Big Data & Analytics

Trending

Trends with increasing attention

▲ 35%	Gamification
▲ 35%	Mobile Payments
▲ 28%	3D Printing

Fading

Trends with decreasing attention

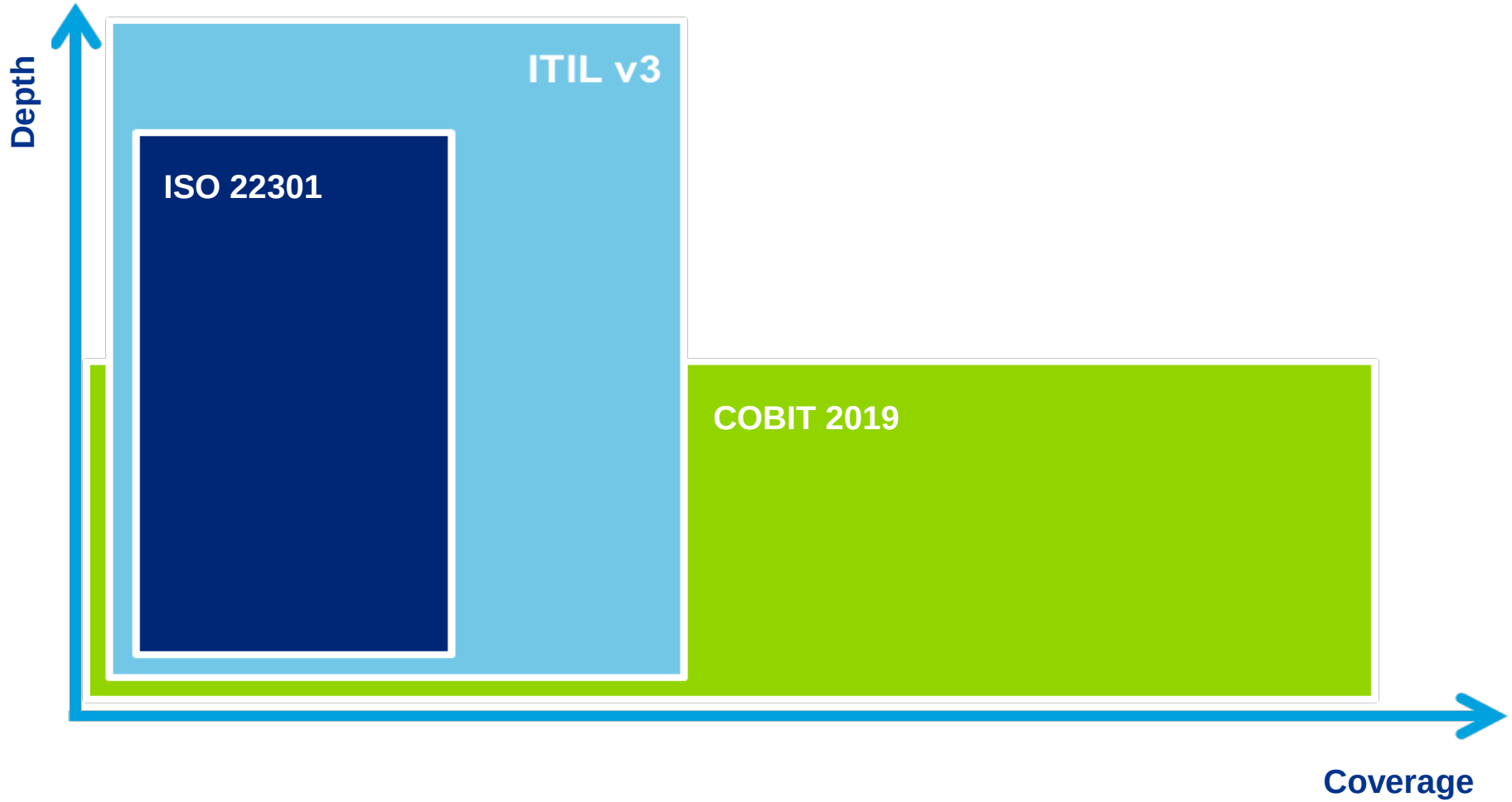
▼ -50%	Quantum Computing
▼ -27%	Autonomous Vehicles
▼ -18%	Speech Analytics

Last update: 14:00

KPMG

Requirements for business continuity

High level comparison of known frameworks



Cobit 2019 includes one process for business continuity

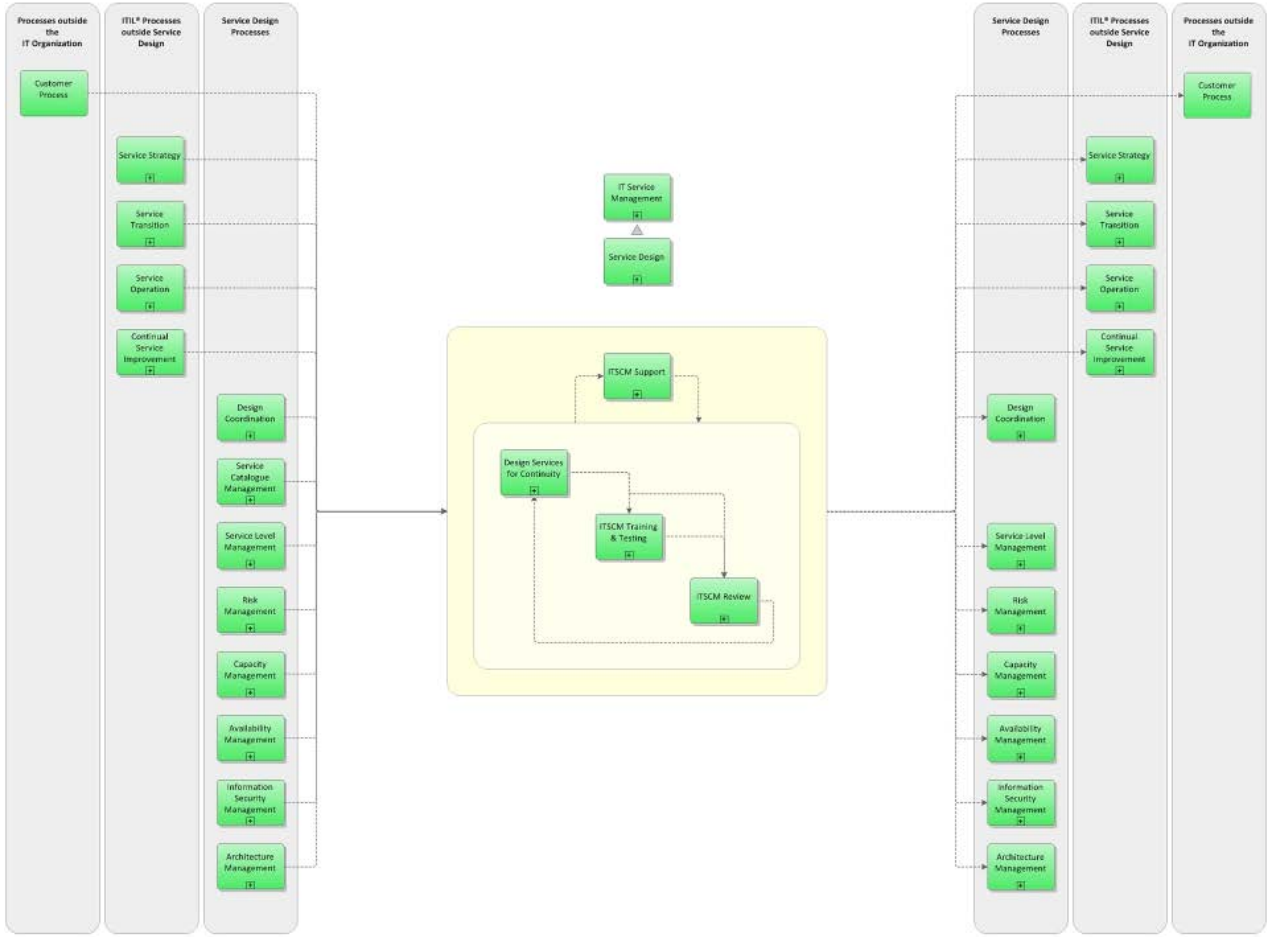
Domain: Deliver, Service and Support Management Objective: DSS04 - Managed Continuity	Focus Area: COBIT Core Model
Description	
Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets and information at a level acceptable to the enterprise.	
Purpose	
Adapt rapidly, continue business operations and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands).	

DSS04.01 Define the business continuity policy, objectives and scope.
DSS04.02 Maintain business resilience.
DSS04.03 Develop and implement a business continuity response.
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).
DSS04.05 Review, maintain and improve the continuity plans.
DSS04.06 Conduct continuity plan training.
DSS04.07 Manage backup arrangements.
DSS04.08 Conduct post-resumption review.

ITIL v3 - IT Service Continuity Management

IT Service Continuity Management (ITSCM) consist of four sub processes:

1. ITSCM Support
2. Design Services for continuity
3. ITSCM Training and Testing
4. ITSCM Review



https://wiki.en.it-processmaps.com/index.php/IT_Service_Continuity_Management

ISO 22300 series

Standards in the area of societal security: i.e. protection of society from and response to incidents, emergencies, and disasters caused by intentional and unintentional human acts, natural hazards, and technical failures

ISO 22300:2012 Societal security – Terminology

ISO 22301:2012 Societal security – Business continuity management systems – Requirements

ISO 22311:2012 Societal security – Video-surveillance – Export interoperability

ISO 22313:2012 Societal security – Business continuity management systems – Guidance

ISO 22315:2014 Societal security – Mass evacuation – Guidelines for planning

ISO 22317:2015 Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)

ISO 22320:2011 Societal security – Emergency management – Requirements for incident response

ISO 22322:2015 Societal security – Emergency management – Guidelines for public warning

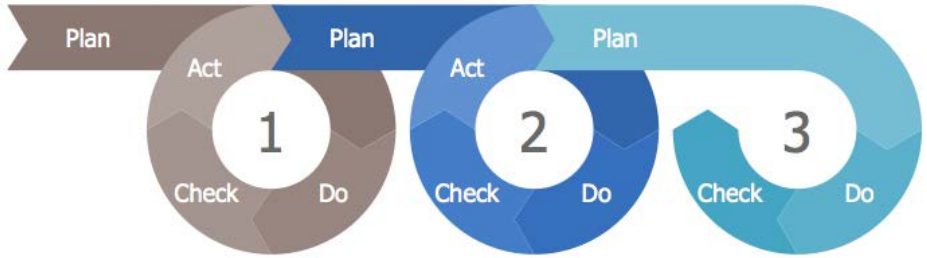
ISO 22324:2015 Societal security – Emergency management – Guidelines for colour-coded alert

ISO 22397:2014 Societal security – Guidelines for establishing partnering arrangements

ISO 22398:2013 Societal security – Guidelines for exercises

Structure and table of content equals to ISO27001

ISO 22301 content



Context of the organisation

Leadership

Commitment
Policy
Roles and responsibilities

Continuity objectives

Planning

Operations

Business impact and risk assessment
Continuity strategies
Plans and procedures
Excercises

Competence
Awareness and communication
Documented information

Support

Performance Evaluation

Monitoring
Audits
Management review

Improvement

National requirements in Finland

Requirements for ICT Contingency Planning

1. **Leadership**
   a. Strategic control
   b. Organisation
   c. Cooperation, communication and reporting

2. **Strategies and operational planning**
   a. Operational planning through risk management
   b. Service continuity planning

3. **People**
   a. Developing expertise and awareness
   b. Management of human resources and tasks

4. **Partnerships and resources**
   a. Contract management
   b. Securing operations in special situations

5. **ICT continuity management**
   a. Lifecycle management of ICT services and systems
   b. Ensuring the continuity of ICT services
   c. Measurement and reporting

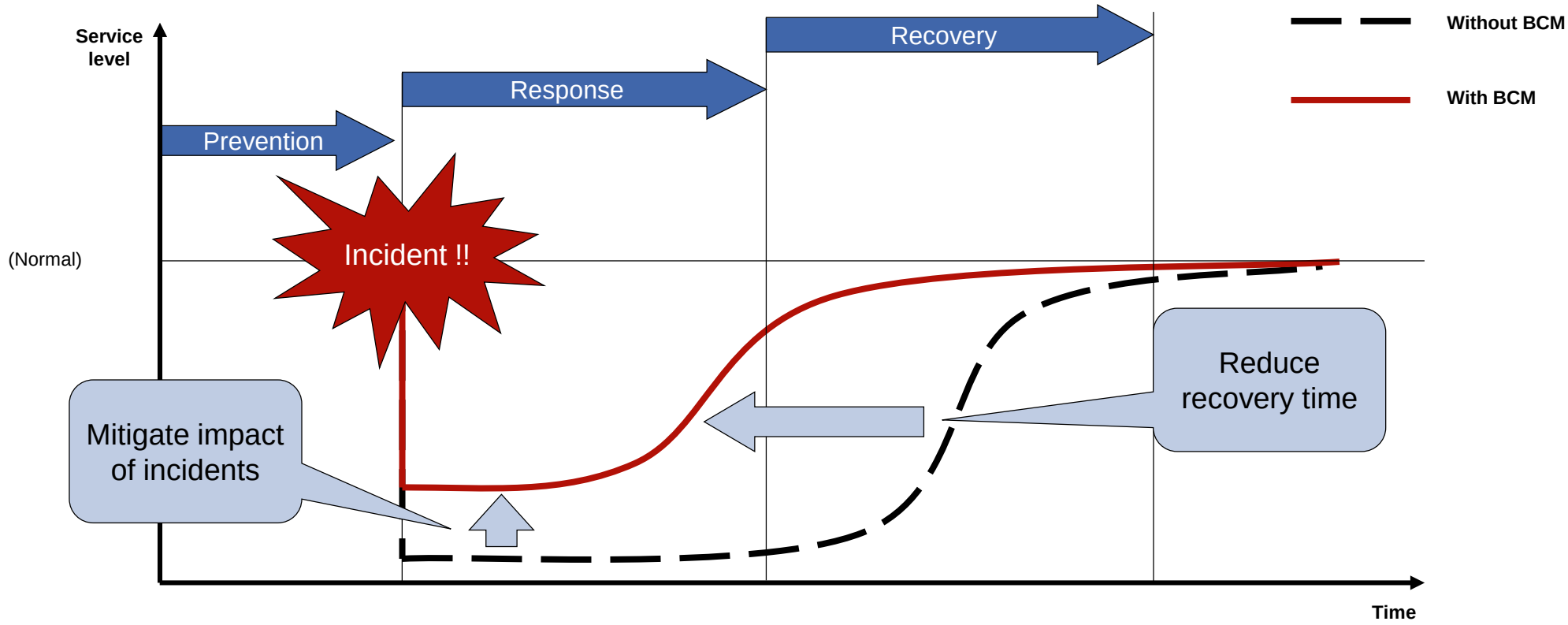
KPMG

Building blocks for business continuity

What is business continuity management?

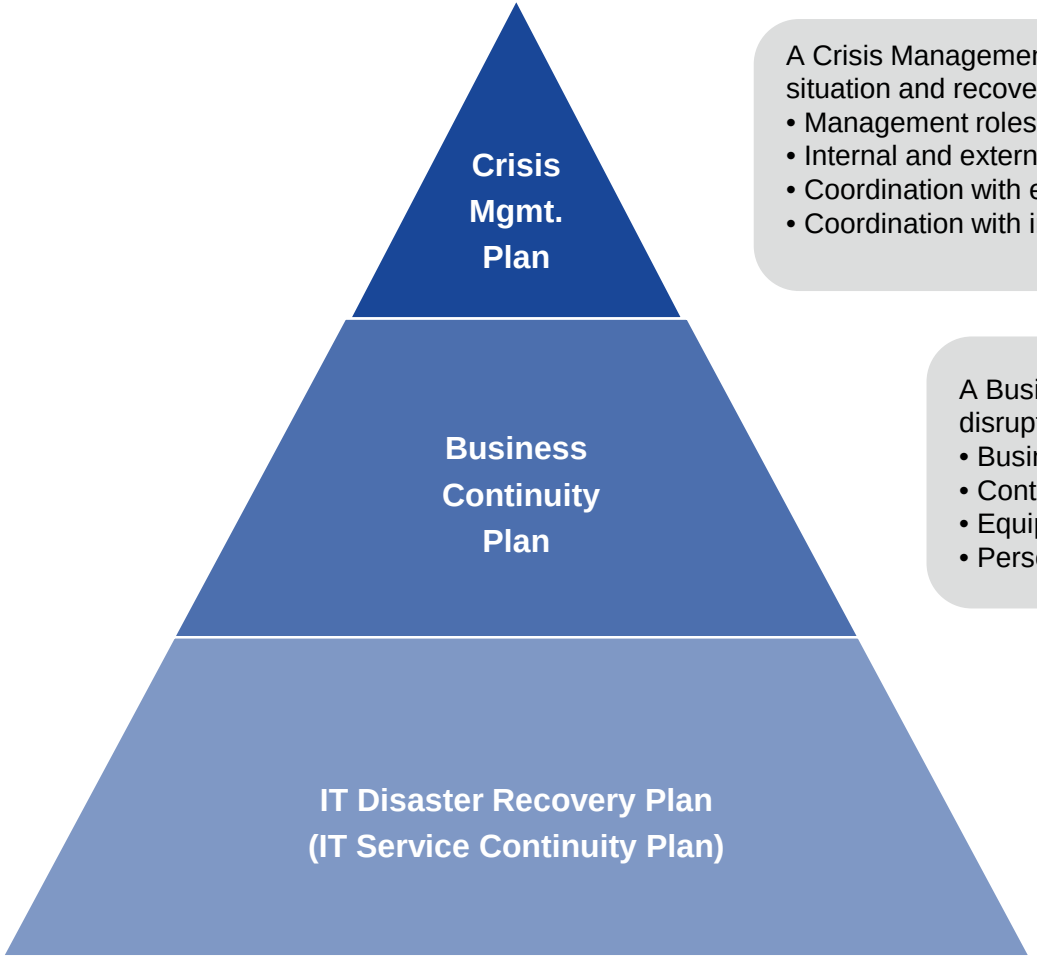
Definition:

“Business Continuity Management (BCM) is an holistic process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause. It provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities.” (Business Continuity Institute, Good Practice Guide 2010)



Business Continuity Management includes appropriate strategies to manage service levels (**mitigate impact**) and reduce time spent on recovery (**reduce recovery time**) following major business disruption.

What is a Business Continuity Management Framework?



A Crisis Management Plan (CMP) outlines the immediate management level response to manage a crisis situation and recover critical operations. CMPs may include:
- Management roles and responsibilities, including escalation procedures
- Internal and external communication strategies, including stakeholder management
- Coordination with external recovery agencies
- Coordination with internal business continuity and recovery teams.

A Business Continuity Plan (BCP) outlines the procedures to follow during a major unanticipated disruptive event. BCPs may include:
- Business recovery strategies (what needs to be performed to continue critical operations)
- Contact lists
- Equipment requirements
- Personnel requirements.

An IT Disaster Recovery Plan (DRP) outlines the specific procedures required to recover or restore critical IT systems. A DRP can be incorporated either as part of a BCP, or more commonly is a separate document.

Steps for effective Business Continuity Management

	Assess (Act)	Design (Plan)	Implement (Do)	Measure (Check)
Objectives	• Understand the key risks, likelihood of occurrence and potential impacts. • Understand the impact of disruptions on business.	• Determine appropriate Business Continuity strategies. • Develop a framework for Business Continuity Management.	• Develop Business Continuity documentation to support continuity of key processes. • Identify and appoint Business Continuity roles.	• Training and awareness of Business Continuity processes. • Validate BCP.
Outcomes	• Business Impact and Risk Assessment report.	• Business Continuity Management strategy. • Business Continuity Management policy and framework.	• Business Continuity Plan. • Crisis Management Plan. • Training pack.	• Test exercise report.

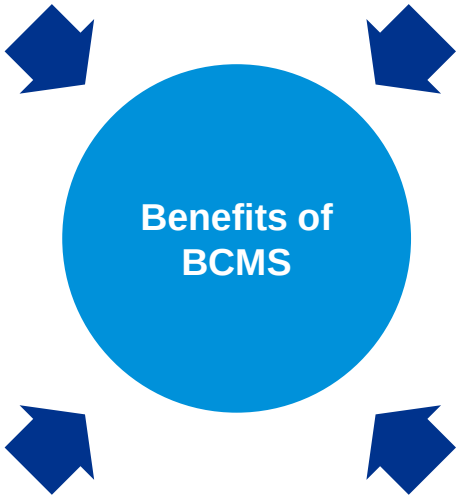
Business Continuity Management system benefits

Business perspective

- supporting its strategic objectives
- creating a competitive advantage
- protecting and enhancing its reputation and credibility
- contributing to organizational resilience

Financial perspective

- making business partners confident in its success
- reducing legal and financial exposure
- reducing direct and indirect costs of disruptions



Perspective of interested parties

- protecting life, property and environment
- considering the expectations of interested parties

Internal processes perspective

- improving its capability to remain effective during disruptions;
- demonstrating proactive control of risks effectively and efficiently;
- addressing operational vulnerabilities

KPMG

Top ten incident responce mistakes

Top 10 incident response mistakes

Plans are not tailored	Organizations should establish policies, processes, and procedures that are tailored to their culture, environment, response personnel, and most importantly, business objectives.
Plans are only used in real-world	Organizations need to put their plans into action with regular frequency before a real incident occurs. Exercise, Exercise, Exercise!
Teams are unable to communicate	A centralized communication dashboard can help limit the disruptions of constant e-mail messaging, which can lead to missed messages or conflicting information.
Teams lack skills, are wrong-sized, or mismanaged	Organizations should closely evaluate the need for additional training. Strong leader should clearly define roles and responsibilities and promote greater collaboration
Help desk activities can destroy critical evidence	Help desk should be trained to capture a memory image of the system in case of malicious code
Tools are inadequate, unmanaged, untested or underutilized	Organizations should maintain an inventory of tools in a centralized location and establish processes to help ensure timely license renewal and functional component upgrades.
Data pertinent to an incident is not readily available	Addressing this issue requires organizations to understand what data sources they have, what data they are capable of producing, and how they manage their data.
There is no “intelligence” in the threat intelligence	Organizations must integrate threat intelligence into incident response
The incident response team lacks authority	Management must fully support the incident response team, its mission, and its activities during an investigation.
Users are unaware of their role in the security posture	Security management team should continuously educate users not only about common exploitation practices, but also about information security’s role within the organization.

https://assets.kpmg/content/dam/kpmg/pdf/2016/04/cyber-incident-response.pdf

KPMG

Case Telia DC

Rough project timeline

Timeline

October-December

- Planning with the client
  - Scoping
  - Management structures
  - Interviews
  - Backgroud work
  - Information gathering
- Documentation
  - Continuity plans
  - Recovery plans

February

- Pre audit
- Gap analysis and development plan

March-April

- Improvements and updates to the documentation and processes based on pre-audit findings

June

- ISO 22301 audit
  - Audit was the first in Finland and test for the auditor
  - Audit process is similar with ISO 27001 (same structure and leadership model)

July

- Telia recieves ISO22301 certification for Helsinki datacenter

August ->

- Ongoing project to maintain certification
- Exercises and tests

KPMG business continuity model

Business Continuity Methodology provides a structured approach to establish and operate a resiliency and recovery capability throughout an organization, minimizing the impact a disruptive event could cause to the company.

Six key activities for each step in the methodology support the development and deployment of a business continuity management program.

Steps include e.g. understanding recovery requirements, developing strategies and plan, and performing regular testing and maintenance.