HSLU Hochschule Luzern

ISROI

Business Continuity Management – Rise Like a Phoenix

ISROI Meeting, May 24, 2024

Prof. em. Dr. rer. nat. Peter E. Fischer
Dipl. Physiker UBT
peter.e.fischer@hslu.ch

4. Juni 2024

FH Zentralschweiz

“Rise Like a Phoenix!”

- “Rise like a Phoenix from the ashes” means to make a comeback after a disaster
- **This is what “Business Continuity Management” is all about**

“Rise Like a Phoenix!”

- “Rise like a Phoenix from the ashes”
- Phoenix was a magical bird in Egyptian mythology.
- It lived for five hundred years before it burns itself on a pyre, and then it is born again from its ashes.
- “Rise like a Phoenix from the ashes” means to make a comeback after a disaster
- Or emerging from a devastating situation with renewed energy and enthusiasm
- **This is what “Business Continuity Management” is all about**

Example – Royal Marsden (2008)

- 100+ firefighters
- 25 fire engines
- 80-90 patients evacuated
- Fire and smoke visible everywhere in London

Example – Royal Marsden (2008)

- More than 100 firefighters in 25 fire engines were deployed on the blaze
- Between 80-90 patients were helped onto the streets whilst the hospital was filled with thick smoke
- The fire could be seen across the London skyline

Example – WannaCry – Cyber Attack

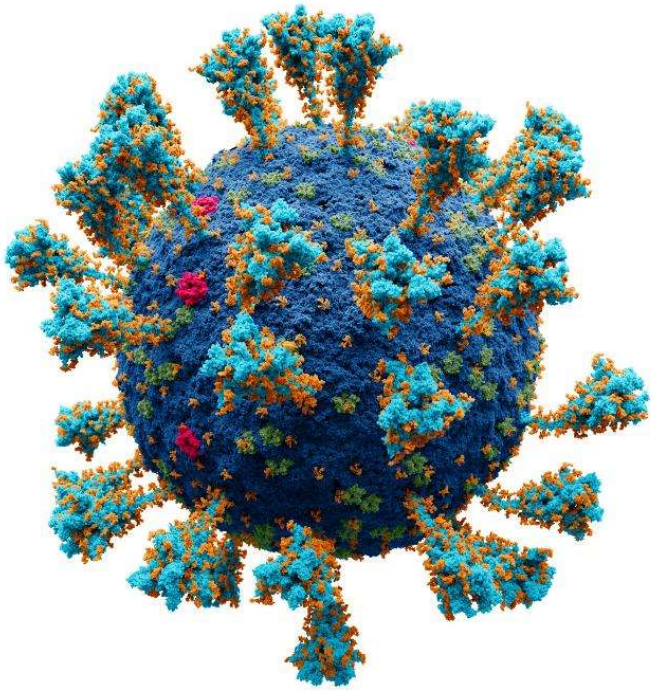
- Friday 12th May 2017 WannaCry outbreak
- Hospitals, lots in England and Scotland
- Key systems, including telephones
- Cancellation of thousands of treatments
- Pen and paper, own mobiles

Example – WannaCry – Cyber Attack

- On Friday 12th May 2017, the NHS, was affected by the WannaCry outbreak, affecting hospitals and GP surgeries across England and Scotland.
- Although the NHS was not specifically targeted, the global cyber-attack highlighted security vulnerabilities and resulted in the cancellation of thousands of appointments and operations.
- Staff were also forced to revert to pen and paper and use their own mobiles after the attack affected key systems, including telephones.
- NHS England reported at least 80 out of the 236 trusts were affected in addition to 603 primary care and other NHS organisations, including 595 GP practices.

Example – Coronavirus (COVID 19)

- Additional to winter "season" on emergency departments
- Staff shortages due to sickness
- Impact on the availability of PPE, e.g. masks
- Supply chain disruption
- Shortage of equipment
- Mental and physical trauma



Fit to NIST Cyber Security Framework – "Resilience"

Risk Management: ID, PR

Business Continuity Management: DE, RS, RC

Risk Management vs. Business Continuity Management (BCM) – "Resilience"

	Risk Management	BCM
Objective	Stability of all processes (**pro-active**)	Fast recovery after failure (**re-active**)
Parameters	Magnitude of damage and frequency / probability of occurence	Magnitude of damage, recovery times and core business processes
Events	**All possible events**	Only significant events with **high impact on core processes**
Impact	All kind of damages from **small to large**	Only events with **disastrous impact**
Intensity	From **slowly creeping in**, developing to high	**Sudden**, grave to disastrous
Methods	**Risk Analysis** (ISO 27005)	**Business Impact Analysis** (BIA, ISO 22031)

Business Continuity Management - Definition

A **holistic** management process that

- identifies potential **threats** to an organisation
- analyses the **impacts** to business operations from those threats
- provides a **framework** for building organisational **resilience**
- establishes the capability of an **effective response**

Objectives:

- **Continuity of core processes after interruption**
- **Avoid further damage**
- **Return to normal operation asap**

ISO22313

Phases

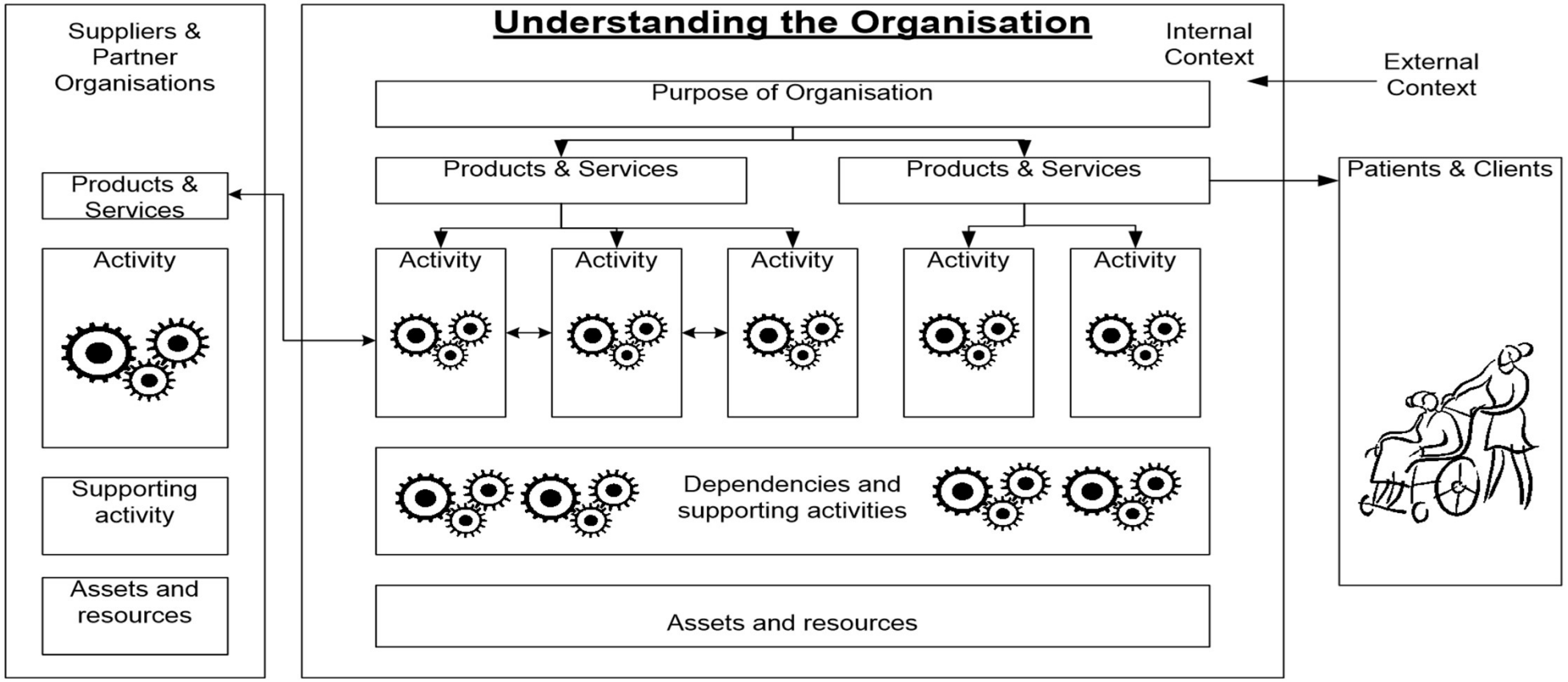
1. Identify **core processes** to be protected and analyse their requirements and dependencies
2. Establish possible emergency **scenarios** and create Business Impact Analysis
3. Define necessary **infrastructure**
4. Plan emergency **readiness**
5. Implement **measures**, stand-by during IT operations
6. Conduct emergency **drills**
7. Kick-in planned measures after an **emergency** occurs
8. **Recover** to normal operation

ISO22313

Elements of BCM 1

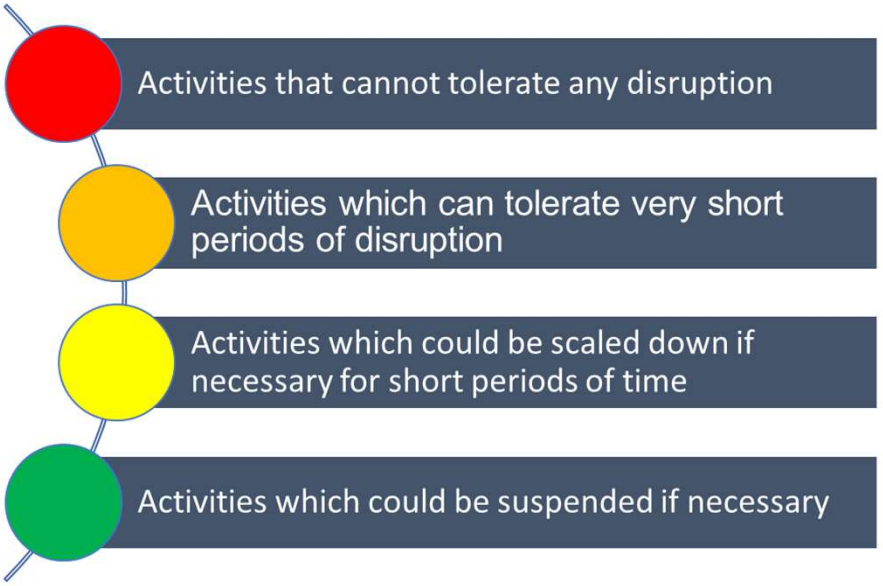
ISO22313

Understanding the Organisation



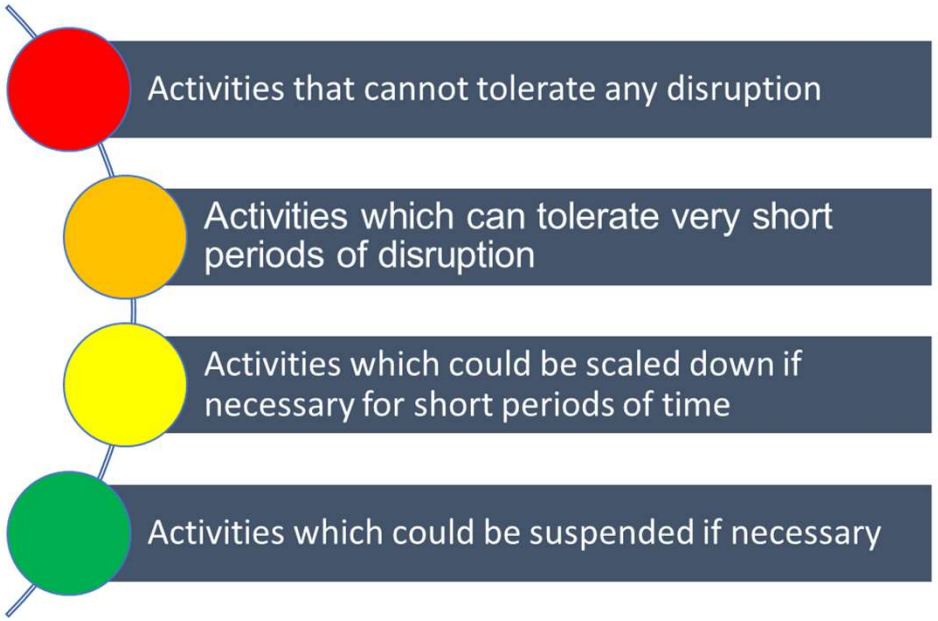
Business Impact Analysis

- After **risk** assessment and treatment
- **Prioritisation** of activities:
  Recovery time objectives (RTO) and
  maximum tolerable period of disruption (MTPoD)
- Identifies the **urgency** of each activity:
  impact over time caused by any disruption
- Identifies business continuity **requirements**:
  to determine appropriate solutions
- Create realistic **scenarios** by assessing possible threats
- Identify resources required for
  maintenance of priority services



Business Impact Analysis

- Follows prior risk assessment and treatment
- Prioritisation of activities:
  including recovery time objectives (RTO) and maximum tolerable period of disruption (MTPoD)
- Identifies the urgency of each activity:
  undertaken by the organisation by assessing the impact over time caused by any potential or actual disruption to this activity on the delivery of products and services
- Identifies business continuity requirements:
  providing information to determine the most appropriate business continuity solutions
- Create realistic scenarios by assessing possible threats
- Identify resources required for maintenance of priority services



Business Impact Analysis

Requirements regarding

- People
- Premises
- Technology
- Information
- Suppliers and partners

Possible **scenarios**

- …
- …
- …

ISO22313

Business Continuity Strategy – Requirements Regarding

People	Premises	Technology	Information	Suppliers and Partners
• What number of staff do you require to carry out critical activities? • What is the minimum staffing level you will need to deliver these? • What skills/level of expertise are required to undertake these activities?	• What locations do your prioritised activities operate from? • What alternative premises do you have? • What machinery, equipment and other facilities are essential?	• Is the service dependant on electrical medical equipment? • What IT is essential to carry out your prioritised activities? • What systems and means of communication are required to carry out your prioritised activities	• What Information is essential to carry out your prioritised activities? • How is this information stored?	• Who are your priority suppliers? • Are key services contracted out? • Do both you and your suppliers/ partners have mutual aid arrangements in please?

Elements of BCM 2

ISO22313

Business Continuity Strategy – Define and Implement

Prevention Strategies

Detail any actions that need to take place as a preventative measure **before** the disaster occurs.

Response Strategies

There should be a detailed response strategy for each department.

Recovery Strategies

After the event has been contained or stabilized, there are necessary steps toward recovery.

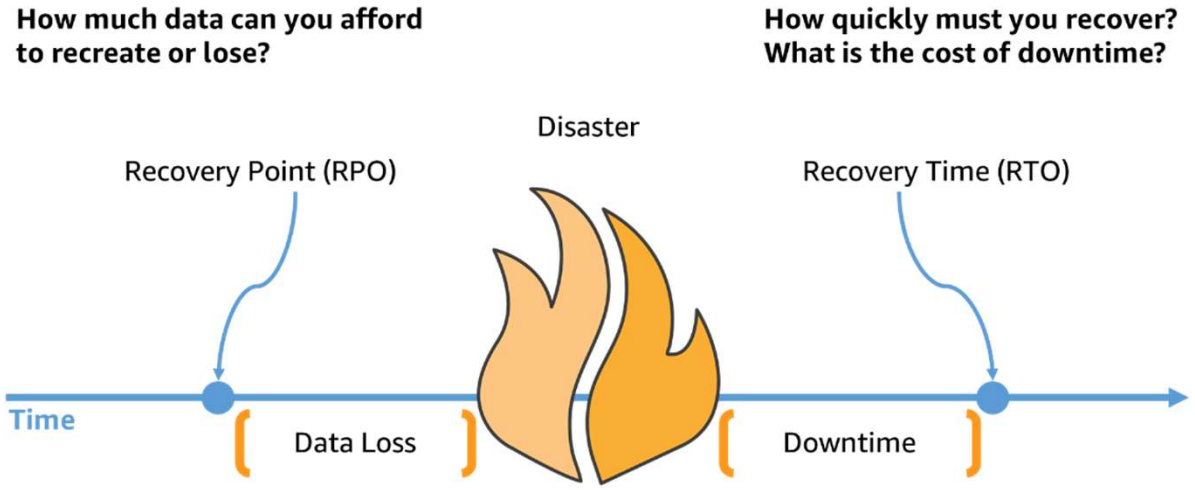
Business Continuity Plan

Elements of BCM 3

Important KPIs

Maximum Tolerable Period of Disruption (MTPoD)

The time it would take for **adverse impacts**, which might arise as a result of not providing a product/service of performing an activity, to **become unacceptable**.



Important KPIs

Recovery Time Objective (RTO)

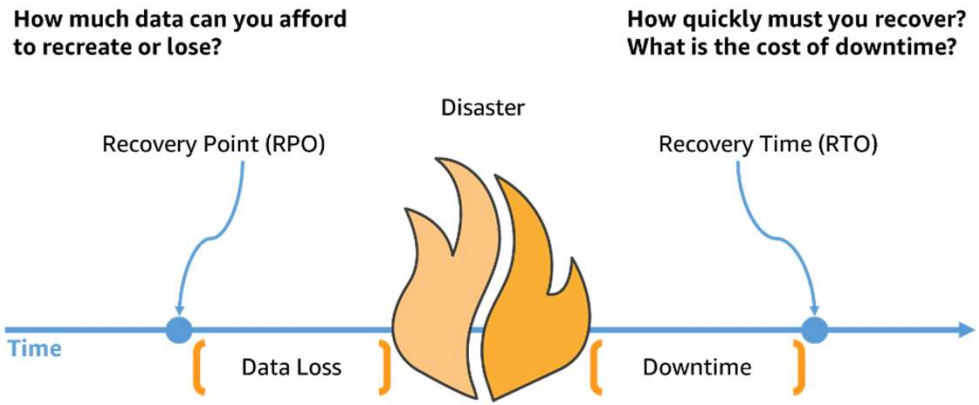
A period of time following an incident within which a product or **service must be resumed**, or activity must be resumed, or resources must be recovered.

Recovery Point Objective (RPO)

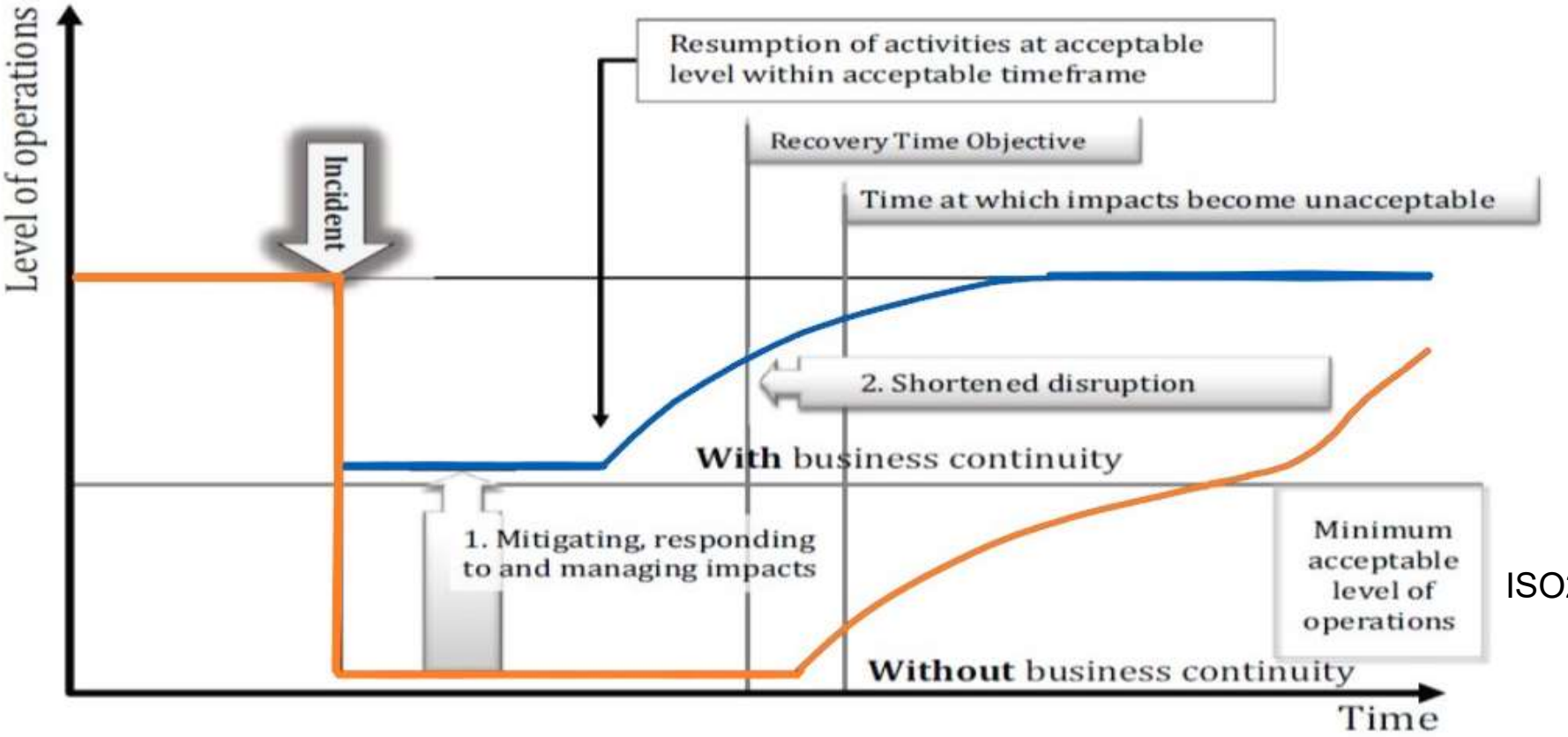
A time-based measurement of the maximum amount of data loss that is tolerable to an organisation.

Maximum Tolerable Period of Disruption (MTPoD)

The time it would take for **adverse impacts**, which might arise as a result of not providing a product/service of performing an activity, to **become unacceptable**.

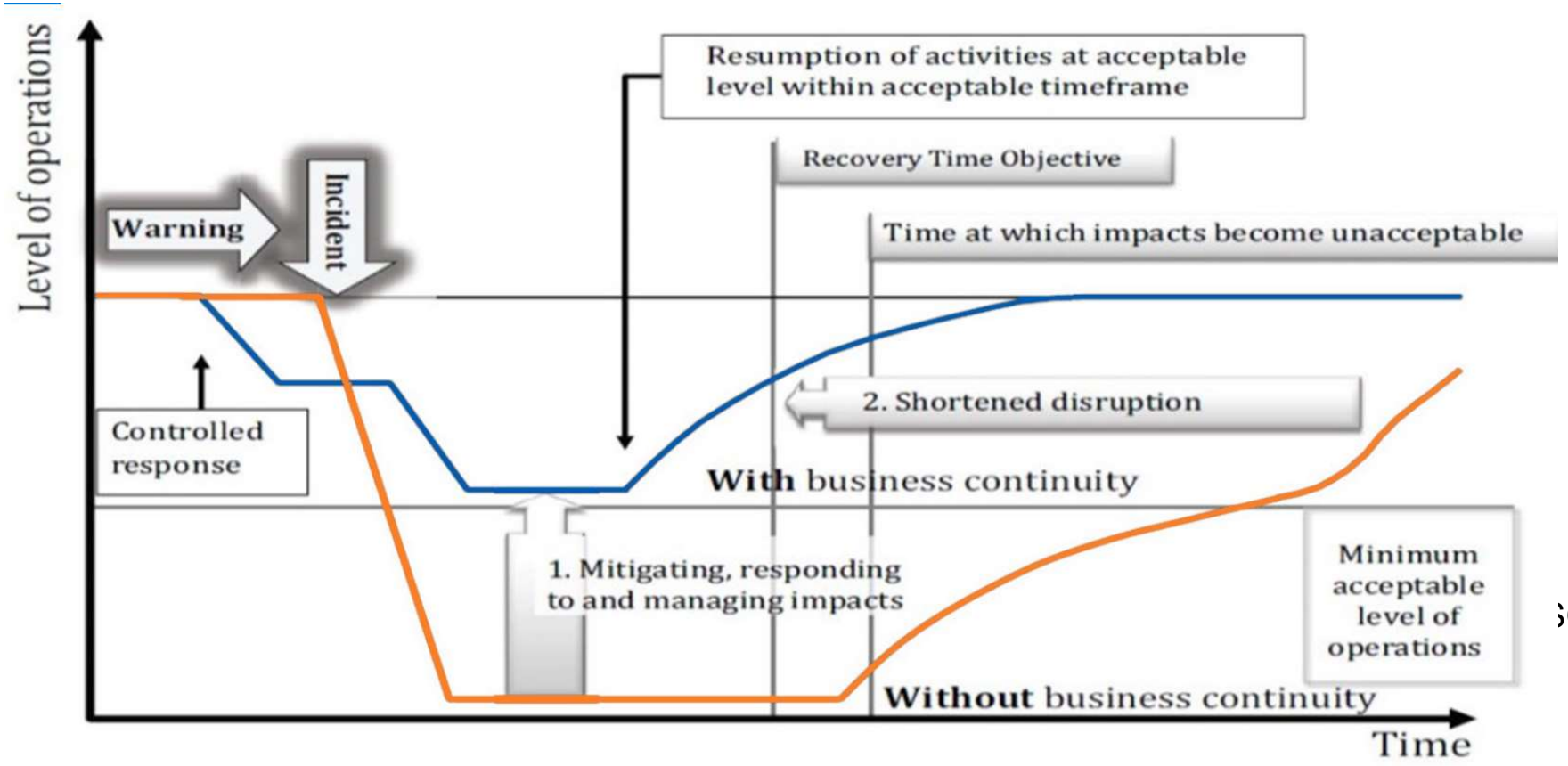


Mitigating Impacts Through Effective Business Continuity: **Sudden** Disruption



ISO22313

Mitigating Impacts Through Effective Business Continuity: **Gradual** Disruption



SO22313

Business Continuity Response Plans

Organisations may have numerous plans.

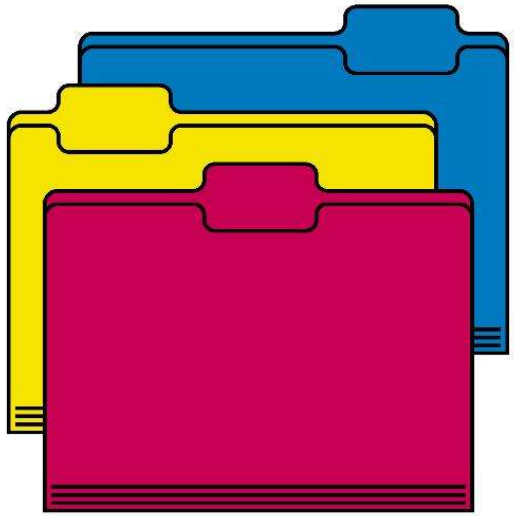
These may include:

- Strategic organisational incident response plan
- Department/service response plans
- Building or site response plans
- Technical response plans for IT or clinical systems

Business Continuity Response Plan Content

The plan should detail the

- **prioritised activities** to be recovered
- **timescales** in which they are to be recovered
- recovery **levels** needed
- **resources** at different points in time
- process for **mobilising** the necessary resources
- storage in a place that's easily **accessible**



Elements of BCM 4

Why Undertake a Business Continuity Exercise?

Validation

- To identify improvement opportunities in existing arrangements

Training

- To develop staff competencies and confidence
  by giving them practice in carrying out their roles in an incident

Testing

- To test existing procedures, plans and systems
  to ensure they function correctly
  and offer the degree of protection expected

Exercising and Testing

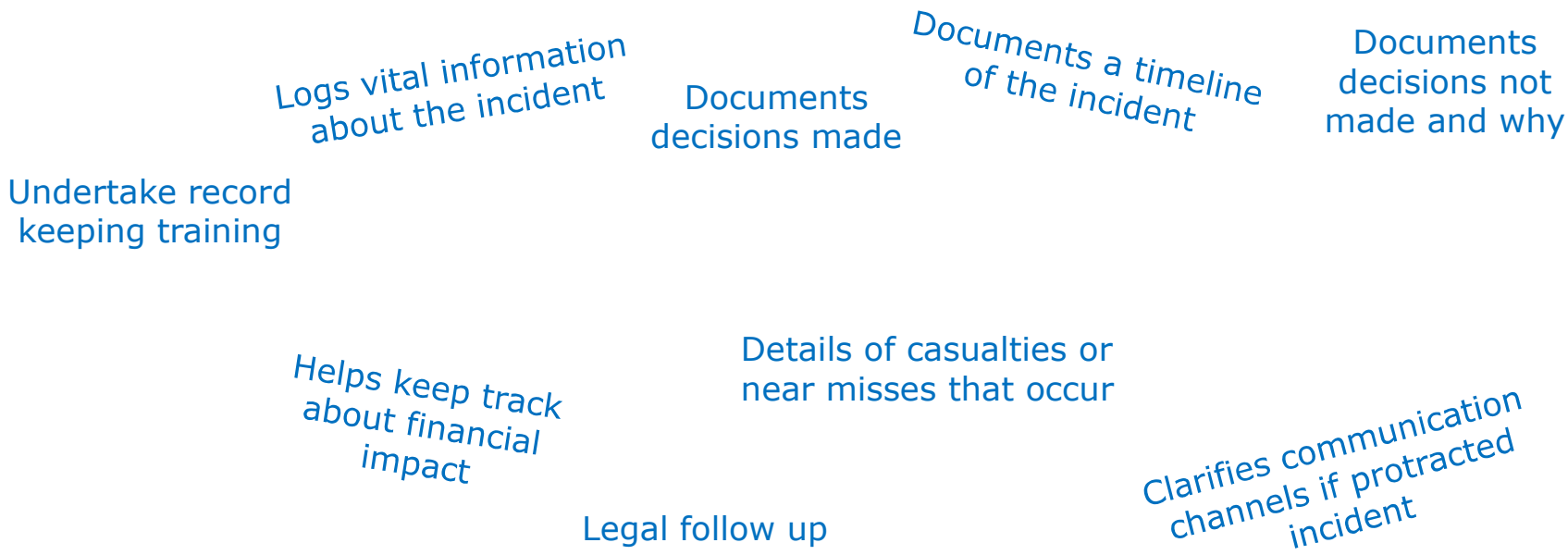
- Exercises provide an opportunity to test plans in order to assess how our plans would stand up in a disruption
- Ensures that plans are fit for purpose
- Identify gaps and learning actions
- Continuous updating of core information i.e. contact lists

Embedding Your Business Continuity Plan

Ensure that business continuity plans are:

- **Communicated** to staff, as well as the staff having the appropriate **experience** and **skills**
- Have **buy in and owned** by the senior management team
- Continually **exercised**
- Version **controlled**, so the correct plan is being followed
- **Documented!**

Why is Record Keeping so Important?

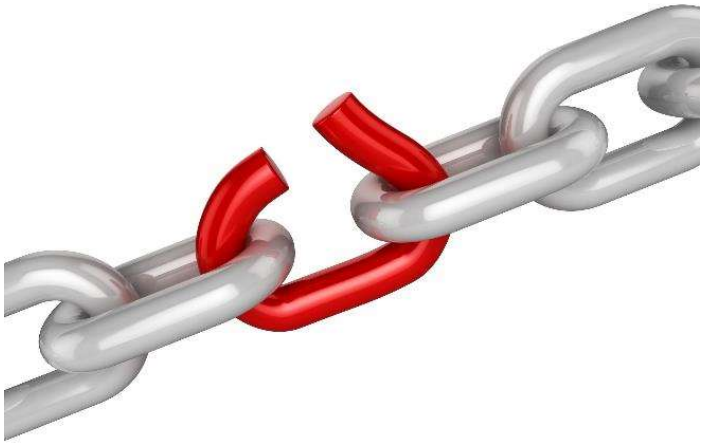


Bring to Life – Rise Like a Phoenix!

- **Education** of employees
- Assignment of **roles** and responsibilities
- Keep all processes and plans **up-to-date**
- Check the **KPIs** like RPO, RTO
- First **test** partially (test or piloting environment)
- Only extend tests to productive environment once you trust your plan

Common Weaknesses Encountered in Emergencies

- Documentation not up-to-date
- Never practiced
- Description too complicated
- Process too cumbersome
- Unavailable during emergencies
- No step-wise restart planned
- Often not taken seriously, must be vigorously enforced!



Summary – Important Aspects

- PDCA-Prozess: **P**lan, **D**o (implementation), **C**heck, **A**ct (continuous improvement process)
- IT Service Continuity Management is IT Readiness for Business Continuity
- Preparation is EVERYTHING!
- Develop, evaluate and prepare for scenarios
- Immediate actions vs. conditional decisions (if … then … else …)
- Awareness, education, tests and exercises
- Communication
- DOCUMENTATION

Q & A

Appendix

- The structure of a Business Continuity Plan
- Five test types
- Reviewing and maintaining Business Continuity Plans
- A video on ITSCM
- The most relevant standards for BCM and ITSCM (IT Readiness for BC)
- The complete set of BCM-related standards
- The Big Picture of Cyber Resilience (around BCM)
- Definitions BC, BCM, BCMS
- Glossary

Business Continuity Response Plan Structure

1. Document control
2. Purpose and scope
3. Document owner and reviewer
4. Roles and responsibilities
5. Plan activation
6. Contact details
7. Incident management structure and plan
8. Action cards
9. Appendences
10. Training and Exercising

Types of Business Continuity Exercises

Discussion based exercise - most cost effective and the least time consuming. Structured events where participants can explore relevant issues and walk through plans in an unpressurised environment. Focus on a specific area for improvement that has been identified.

Table-top exercise - Discussion is based on a relevant scenario, run in 'real time' or may include 'time jumps' to allow different phases of the scenario to be exercised. Participants are expected to be familiar with the plans being exercised and are required to demonstrate how these plans work as the scenario unfolds

Command post exercise - Involve management teams at a strategic, tactical or operational level. Participants can be located across the whole organisation from their usual day to day locations. In these exercises, participants are given information in a way that simulates a real incident.

Live exercise - From a small-scale rehearsal of one component of the response, for example evacuation, through to a full-scale rehearsal of the whole organisation and potentially participating interested parties. Live exercises are designed to include everyone likely to be involved in that part of the response.

Test - A unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned. It is usually applied to equipment, recovery procedures or technology, not to individuals.

Reviewing Business Continuity

Plans should be reviewed and updated when:

- Changes to key staff or partners take place
- The organisation is restructured
- Prioritised activity is delivered differently
- Change to the external environment e.g.. statutory change, NHS England requirement
- Following lessons identified from an incident or exercise
- As a result of a debrief
- At agreed periodic intervals

Maintaining Business Continuity

The maintenance programme should:

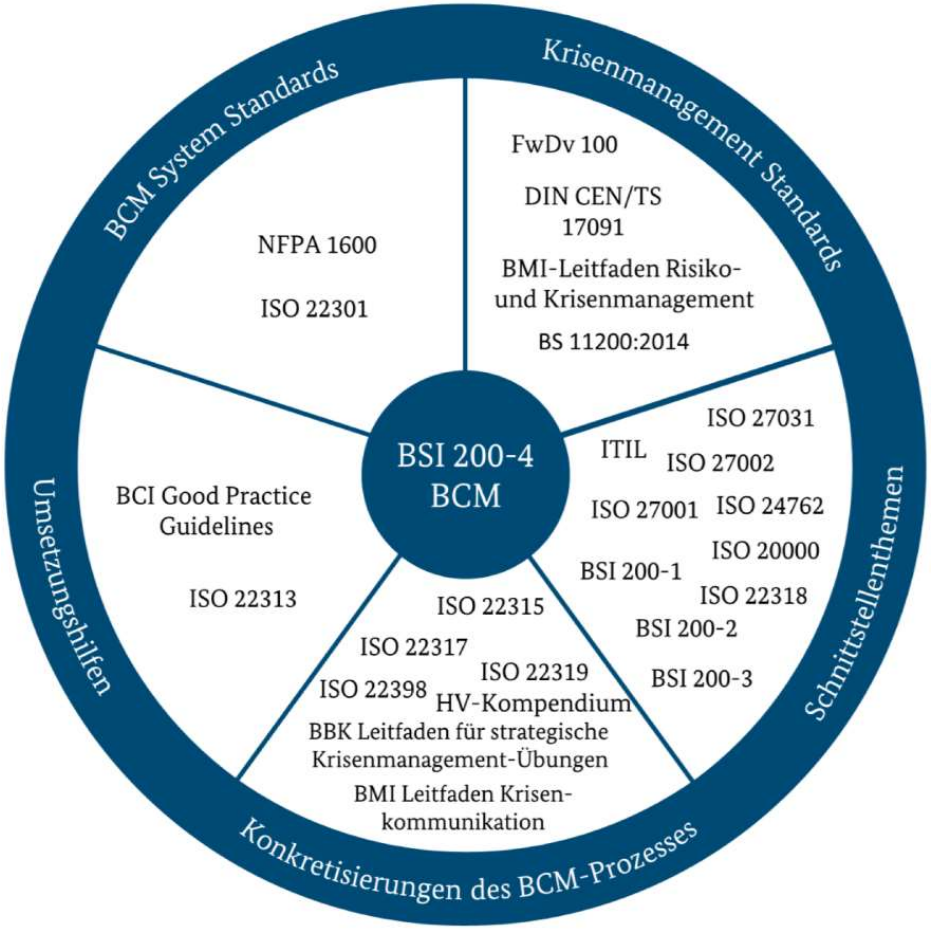
- ensure that there is an on-going programme for business continuity training and awareness
- ensure that any changes that impact on business continuity are reviewed
- identify any new products and services, and their dependent activities that need to be included in the business continuity management system
- ensure that the business continuity plans remains effective, fit for purpose and up to date
- enable existing exercise schedules to be modified when there has been a significant change in any of the business continuity processes

Video – Explanation of ITSCM https://youtu.be/izQ98tRCbdg

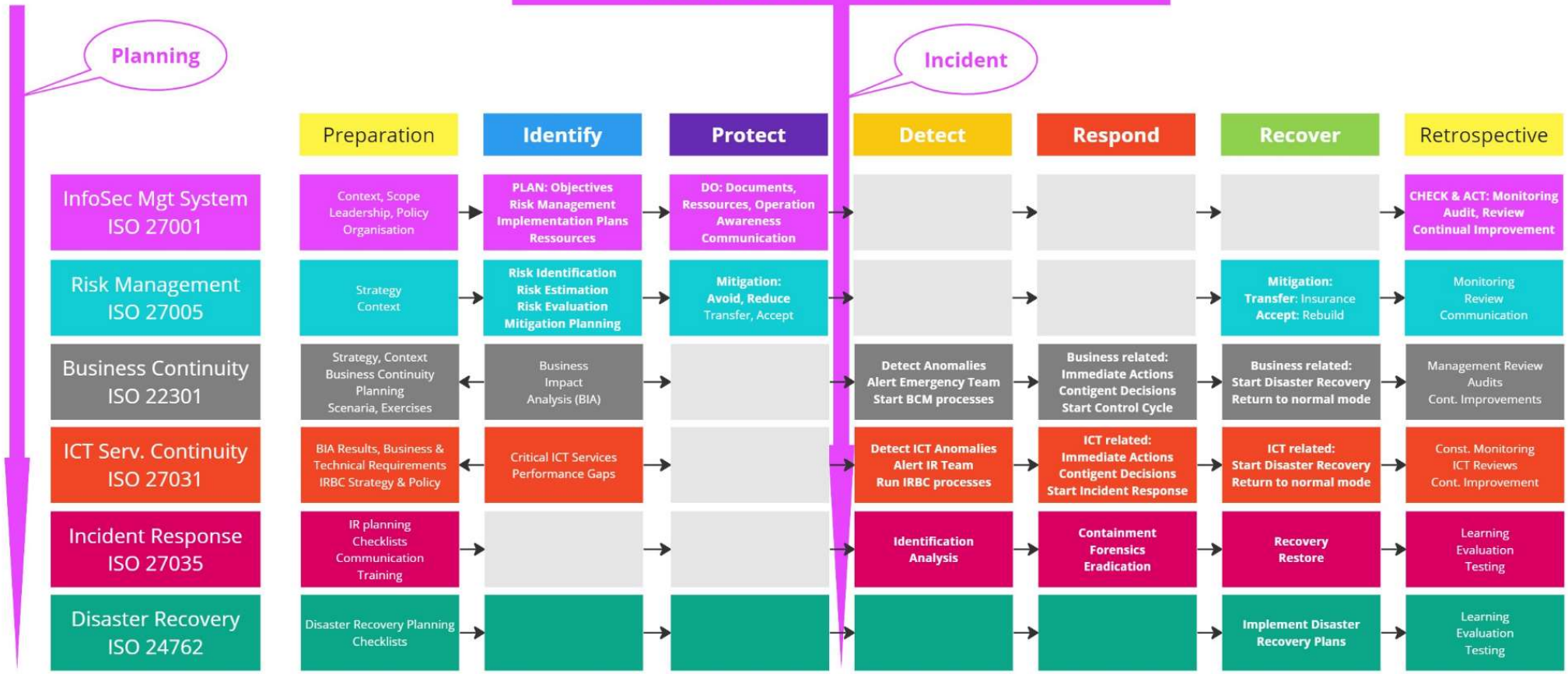
Sources for BCM and ITSCM

- ISO 22301: Security and Resilience – BCMS – Requirements
- ISO 22313: Societal security — Business continuity management systems — Guidance
- ISO 27031: ICT Readiness for Business Continuity
- ISO 24762: ICT Disaster Recovery Services
- ITIL Service Delivery Prozess (see Availability Management, Capacity Management)
- BSI 200-4: 2.4.2, by German BSI, good framework for BCM)

Standards for BCM



Cyber Resilience Management - Big Picture
(acc. NIST CSFW & ISO Stds.)



boldtype: Focus

16.04.2024

Definitions – ISO 22301:2019

Business Continuity

The capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Business Continuity Management

A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Business continuity management system

Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

Business Continuity Management System ISO 22301 / 22313 (social security)

- A business continuity management system emphasises the importance of
- Understanding the organisation’s needs and the necessity for establishing a business continuity management policy and objectives
- Implementing and operating controls and measures for managing an organisation’s overall capability to manage disruptive incidents
- Monitoring and reviewing the performance and effectiveness of BCMS, and
- Continual improvement based on management of objectives

Glossary

- BCM: Business Continuity Management: focus business, costs, core processes
- BCP: Business Continuity Planning: the planning phase of the PDCA process
- BIA: Business Impact Analysis: impact assessment for core business processes based on emergency scenarios
- CIA: Confidentiality, Integrity, Availability, plus: Authenticity und Non-Repudiation – basic InfoSec objectives
- Event, Alarm / Alert, Incident, Emergency, Crisis: Increasing severity along thresholds
- ITSCM, IT-SCM, IRBC: IT Service Continuity Management or IT Readiness for Business Continuity
- Major Incident: An emergency in the IT realm
- PDCA: Plan, Do, Check, Act – simple process model, used in many ISO standards