

Information and Communications Security WS 24/25

Guest Lecture GL1

Information Security

19th November 2024, Frankfurt

Guest Lecture GL1: 19.11.2024, 10:15-11:45, HZ7
Exercise GL1: 19.11.2024, 16:15-17:45, HZ7

Michael Schmid
michael.schmid@m-chair.de
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de



Michael Schmid (Dipl. Inf., MBA, CISM, ITIL, BSIG §8a, ISO Lead Auditor)

- Since 2023 Senior Manager Cyber Security Regulations @Lufthansa Group
- Deputy CISO @Hubert Burda Media Holding KG (2012-2023)
- Since 2017 PhD student @m-chair
- University Lecturer & Scientific Reviewer
- > 15 years experience in the field of IT / Information Security
- Areas of focus: ISMS, IT Compliance & Governance and Risk Management, Regulations
- Active participation in (inter)national committees: IATA, ICAO, A-ISAC, A4E, BDL, UPKRITIS, ISACA, GI, CAST



- I. Information Security
- II. Information Security Management System
- III. Risk Management
- IV. Incident Management
- V. Business Continuity Management
- VI. Information Security Measurement
- VII. Further Information Security processes
- VIII. Literature

- I. Information Security**
- II. Information Security Management System
- III. Risk Management
- IV. Incident Management
- V. Business Continuity Management
- VI. Information Security Measurement
- VII. Further Information Security processes
- VIII. Literature

I. Information Security



[Slido](#)



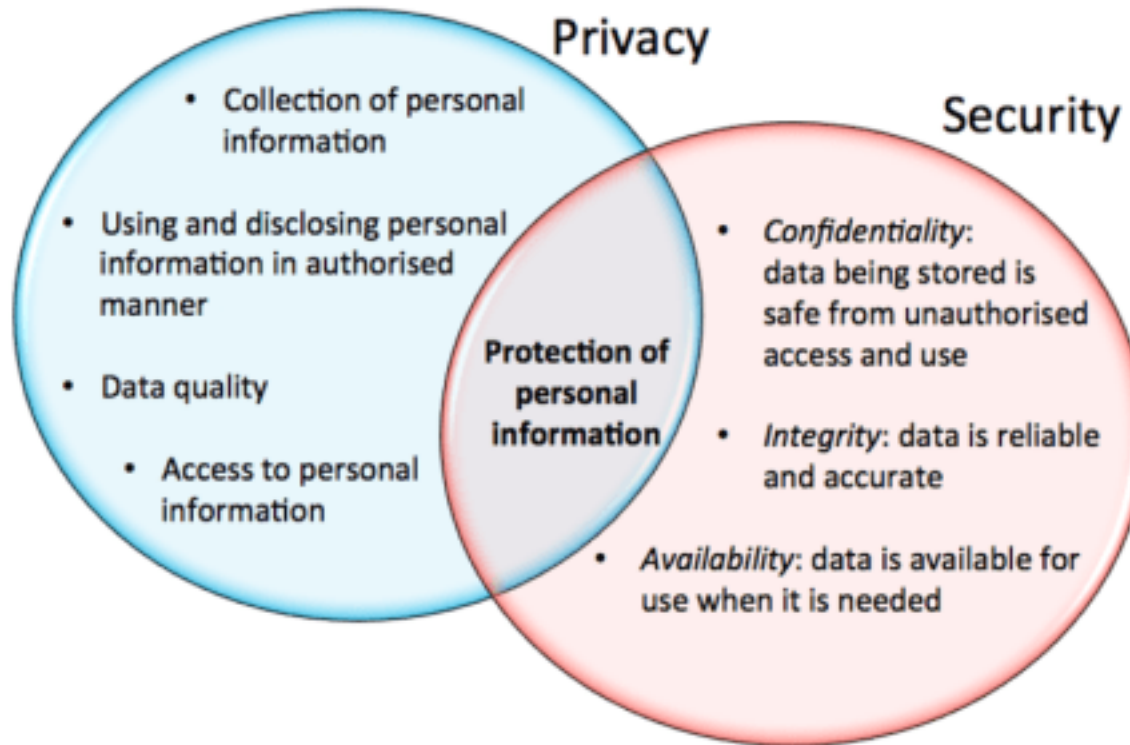
Join at
slido.com
#3369 085



What does information security mean to you?

① Start presenting to display the poll results on this slide.

Privacy vs. Security

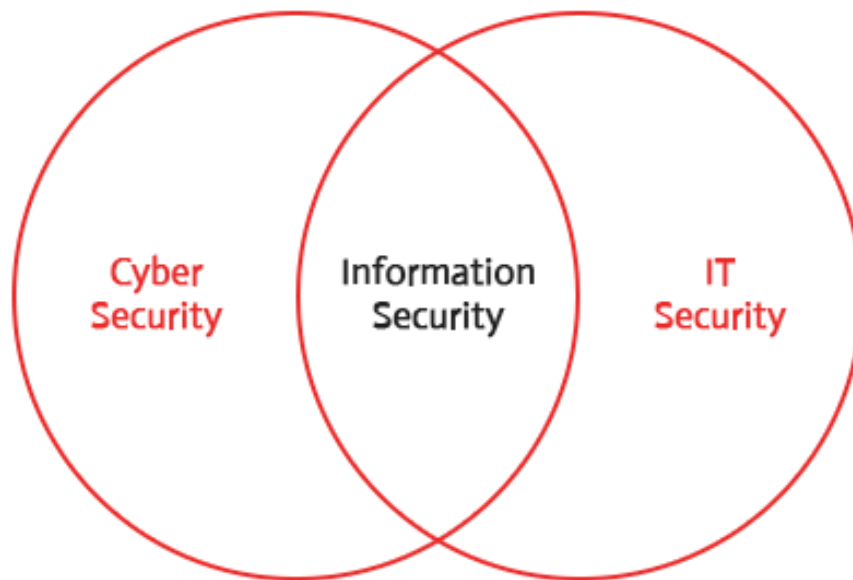


CIA vs. Information security?



I. Information Security

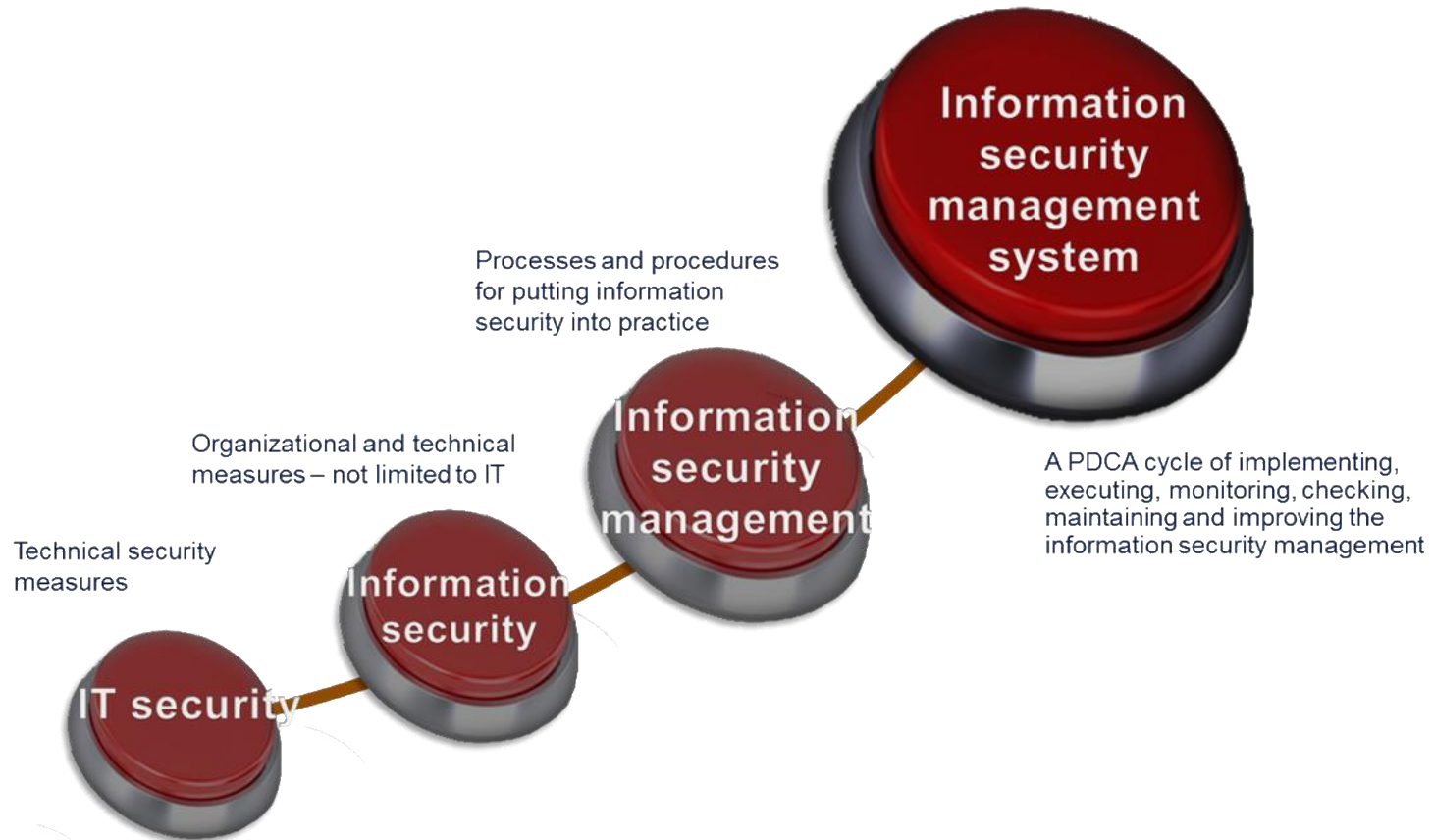
Cyber vs. Information vs. IT Security



- I. Information Security
- II. Information Security Management System**
- III. Risk Management
- IV. Incident Management
- V. Business Continuity Management
- VI. Information Security Measurement
- VII. Further Information Security processes
- VIII. Literature

II. Information Security Management System

From IT security to an Information security management system



II. Information Security Management System

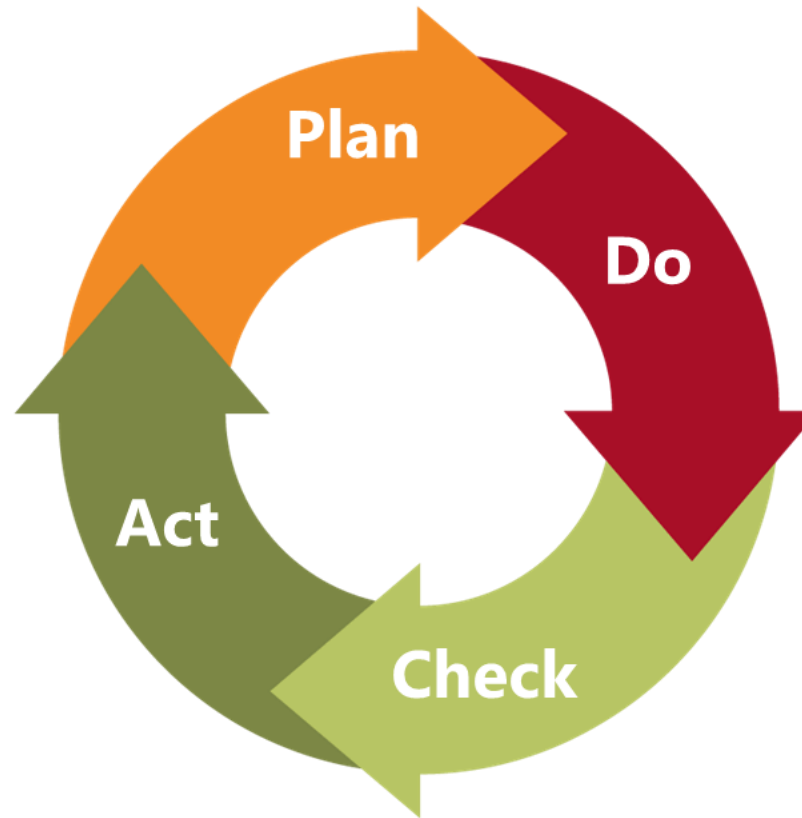


II. Information Security Management System

ISO/IEC 27001:2013 is the internationally recognised management system standard for information security.



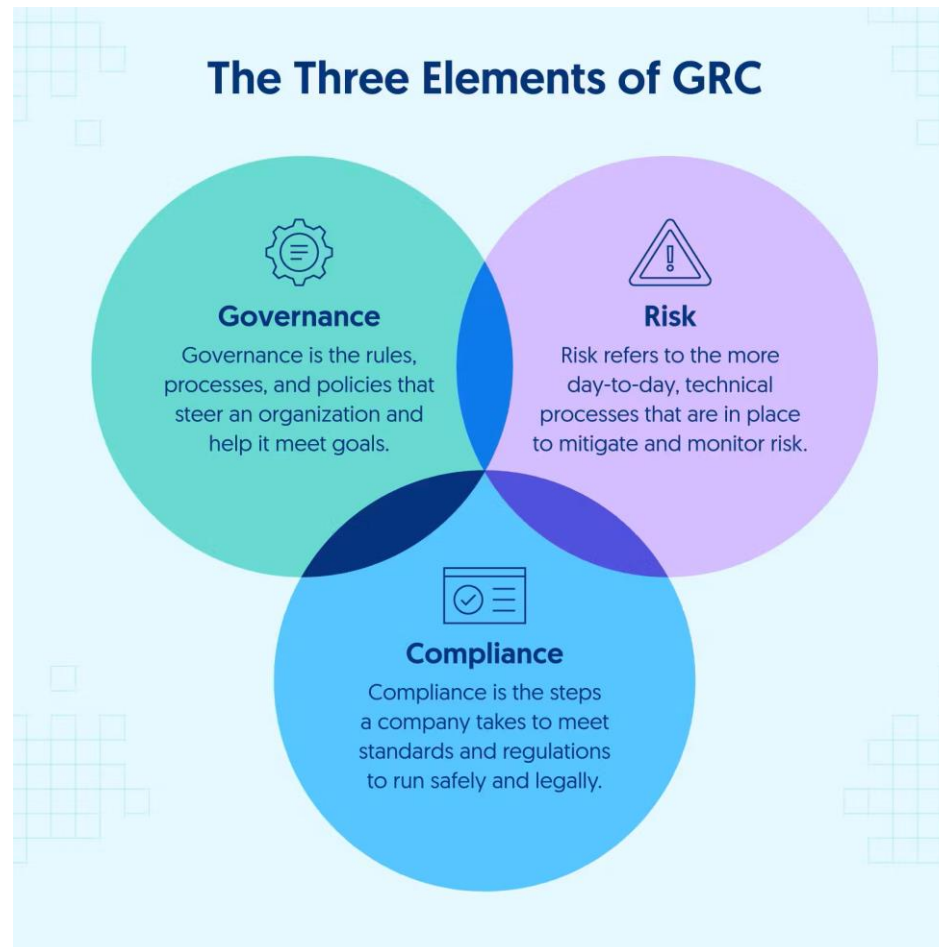
PDCA or Demin circle

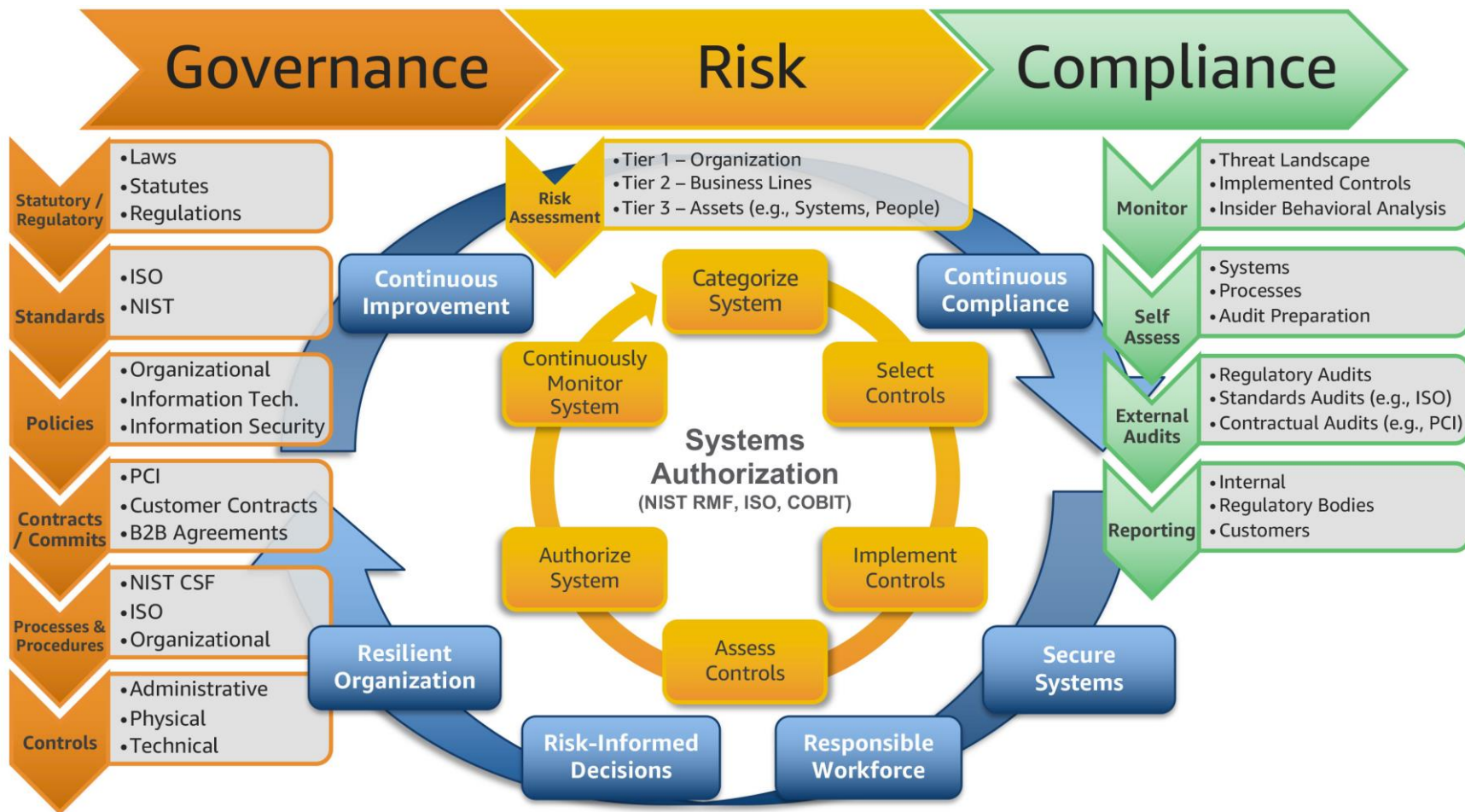


- I. Information Security
- II. Information Security Management System
- III. Risk Management**
- IV. Incident Management
- V. Business Continuity Management
- VI. Information Security Measurement
- VII. Further Information Security processes
- VIII. Literature



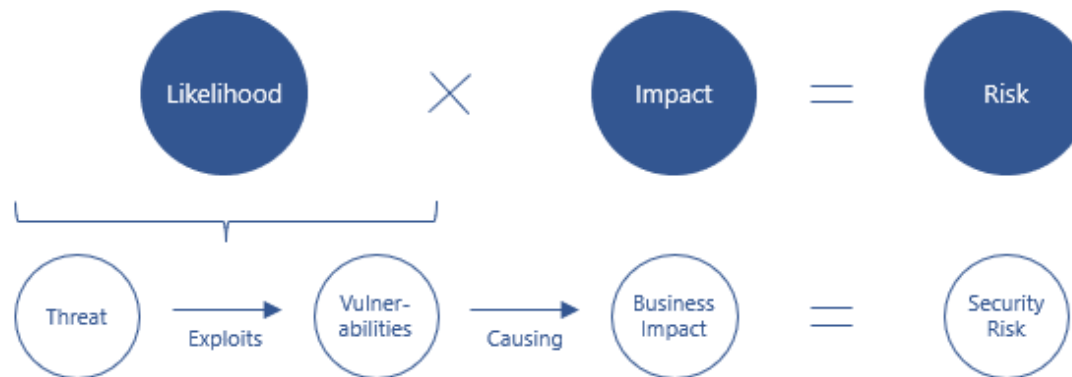
Governance, Risk management and Compliance (GRC)



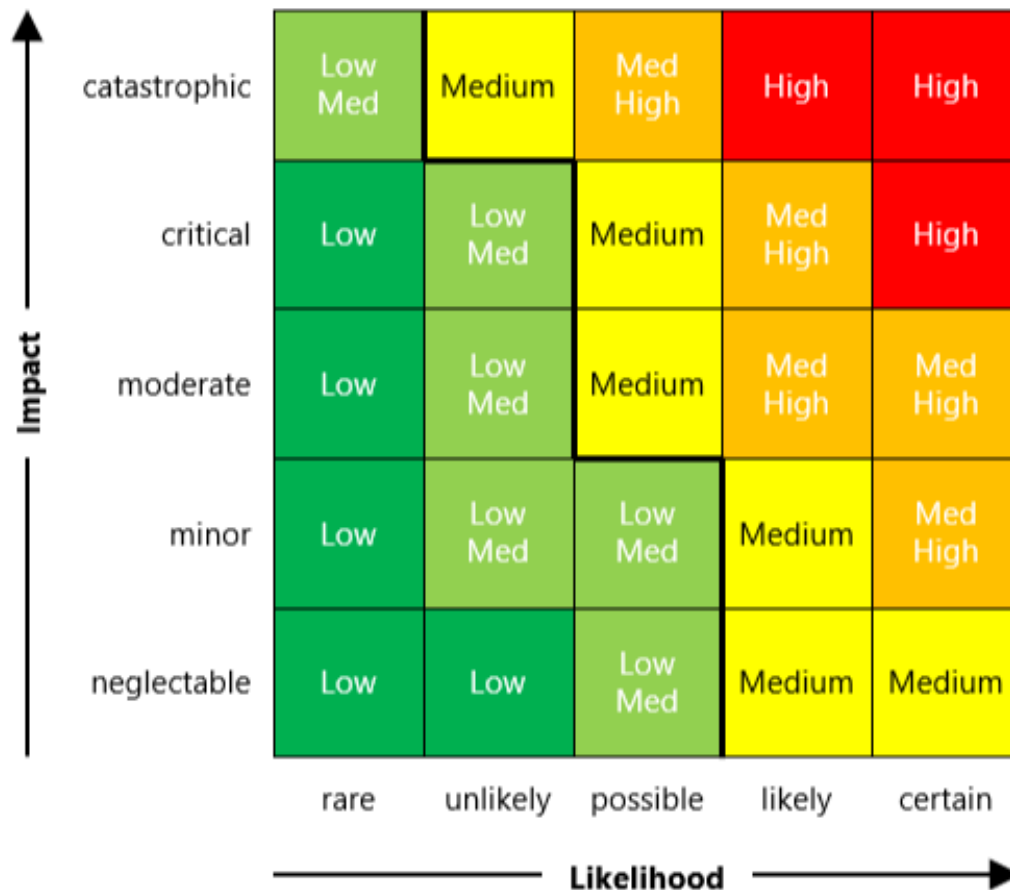


Risk management

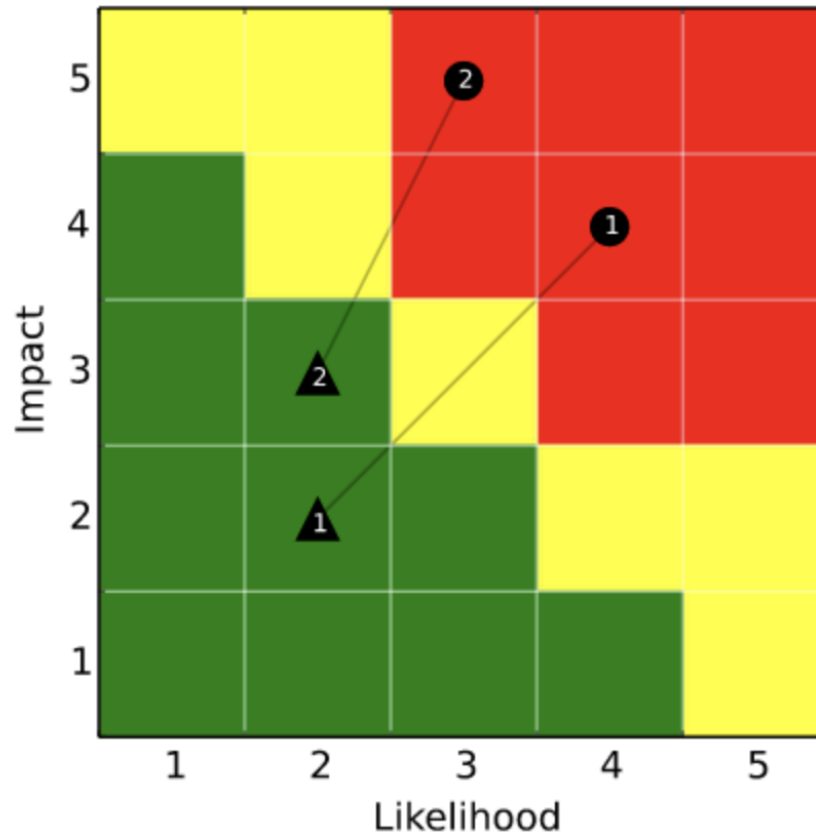
Risk is expressed as a combination of the likelihood of an event occurring and the impact on the business expressed in the equation:



Risk matrix

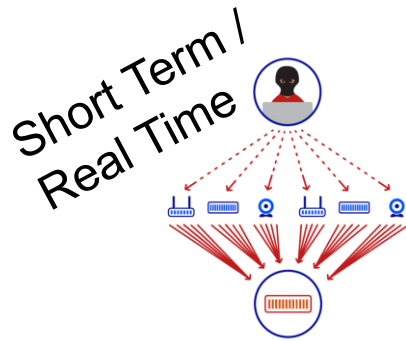


Risk matrix with and without measures



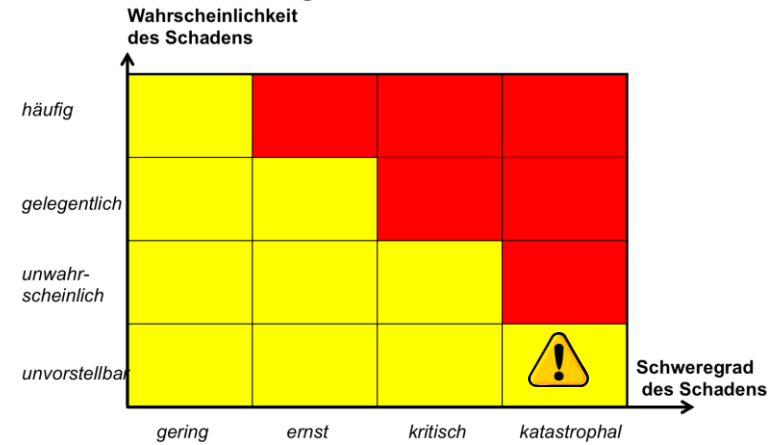
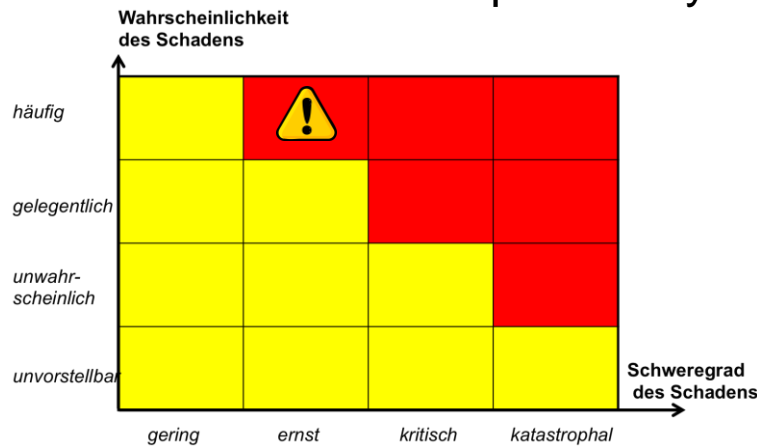
III. Risk Management

Threat + vulnerability = risk



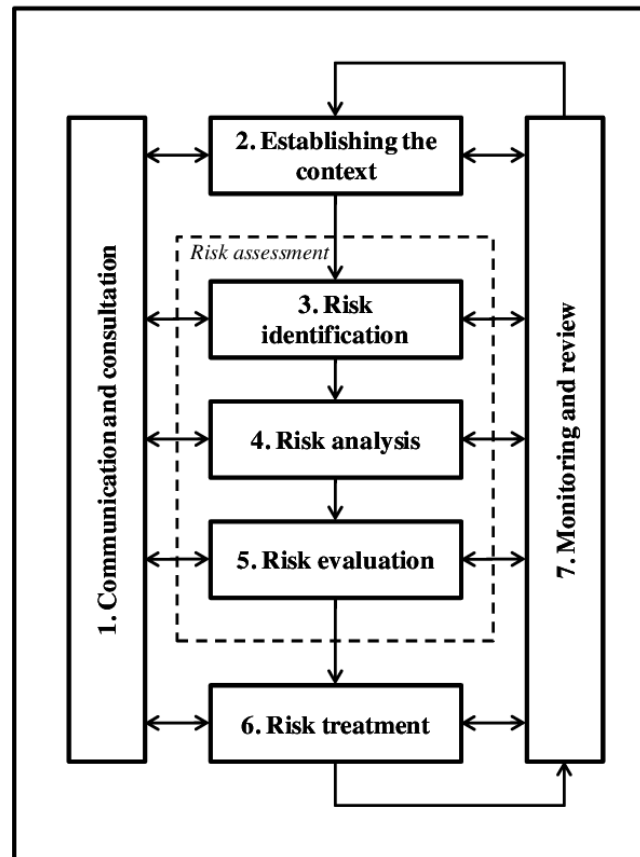
Long Term

Risk matrix = probability of occurrence + damage



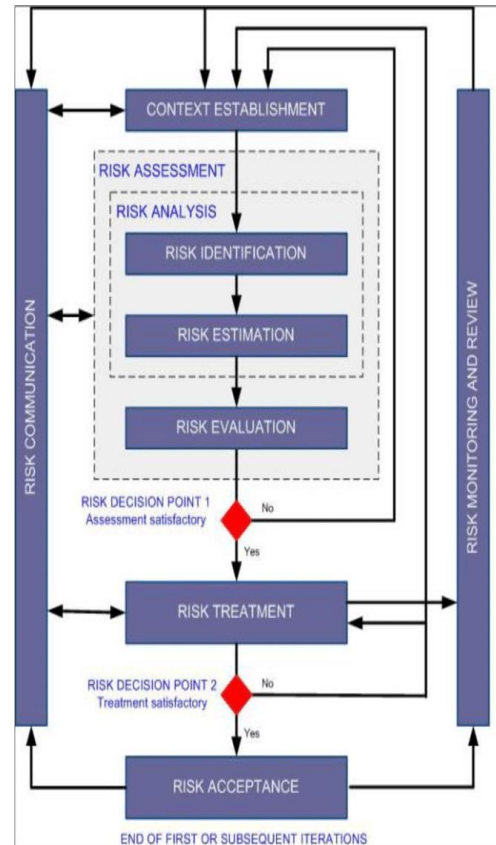
ISO 31000:2018 – provides principles and generic guidelines on managing risks faced by organizations

Risk management process

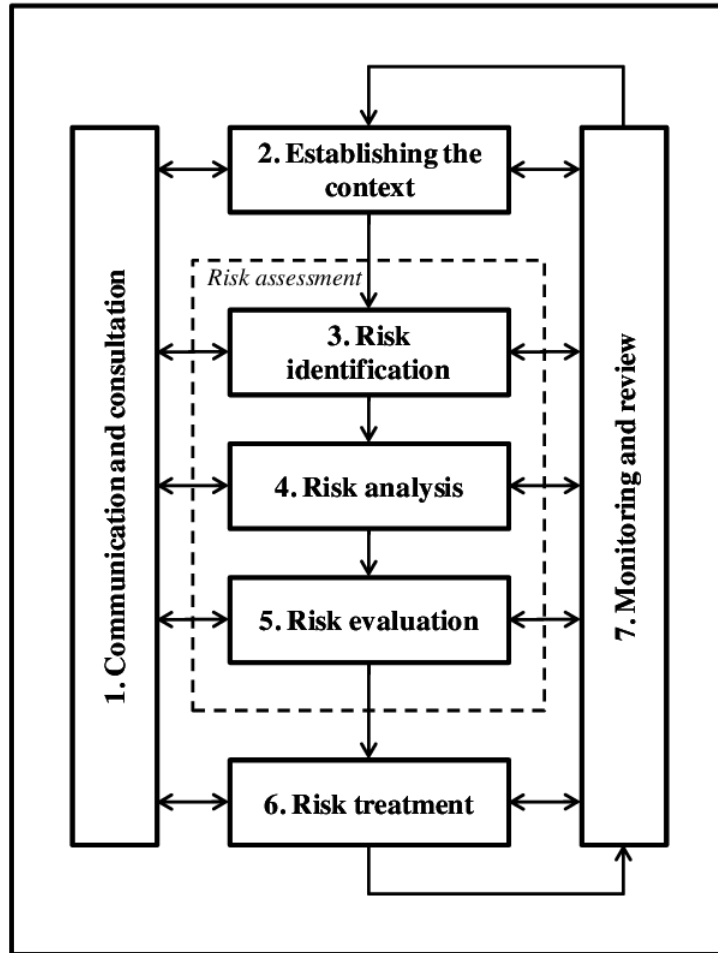


ISO/IEC 27005:2018 - provides guidelines and techniques for managing **information** security risks

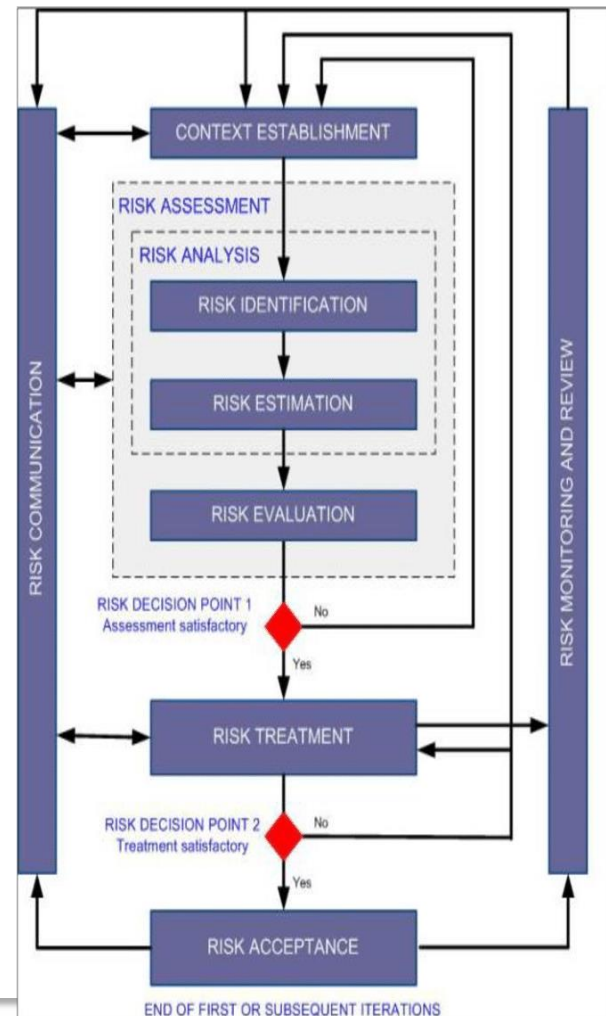
Risk management process



ISO 31000:2018



ISO/IEC 27005:2018



Risk treatment options

1. Avoidance You can choose not to take on the risk by avoiding the actions that cause the risk.
2. Reduction You can take mitigation actions that reduce the risk. For example, wearing a life jacket when you swim.
3. Transfer You can transfer all or part of the risk to a third party. The two main types of transfer are insurance and a company may choose to transfer a collection of project risks by outsourcing the project.
4. Acceptance Risk acceptance, also known as risk retention, is choosing to face a risk. In general, it is impossible to pro enjoy an active life without choosing to take on risk.

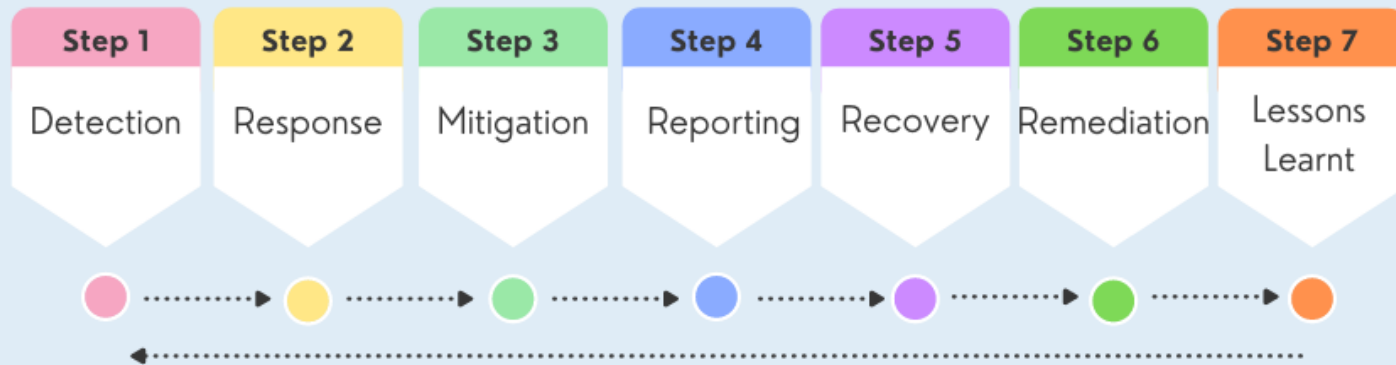
=> Residual risk ✓

- I. Information Security
- II. Information Security Management System
- III. Risk Management
- IV. Incident Management**
- V. Business Continuity & Incident Management
- VI. Information Security Measurement
- VII. Further Information Security processes
- VIII. Literature

IV. Incident Management



Incident Management Steps

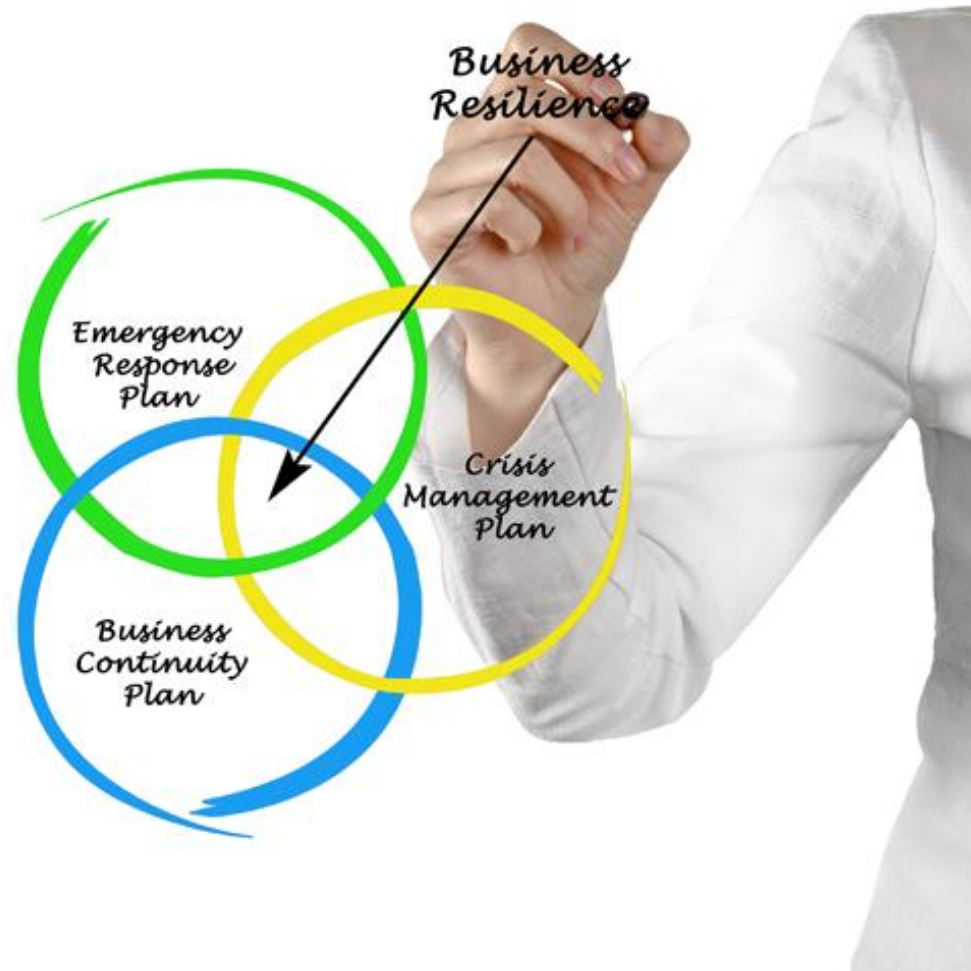


IV. Incident Management

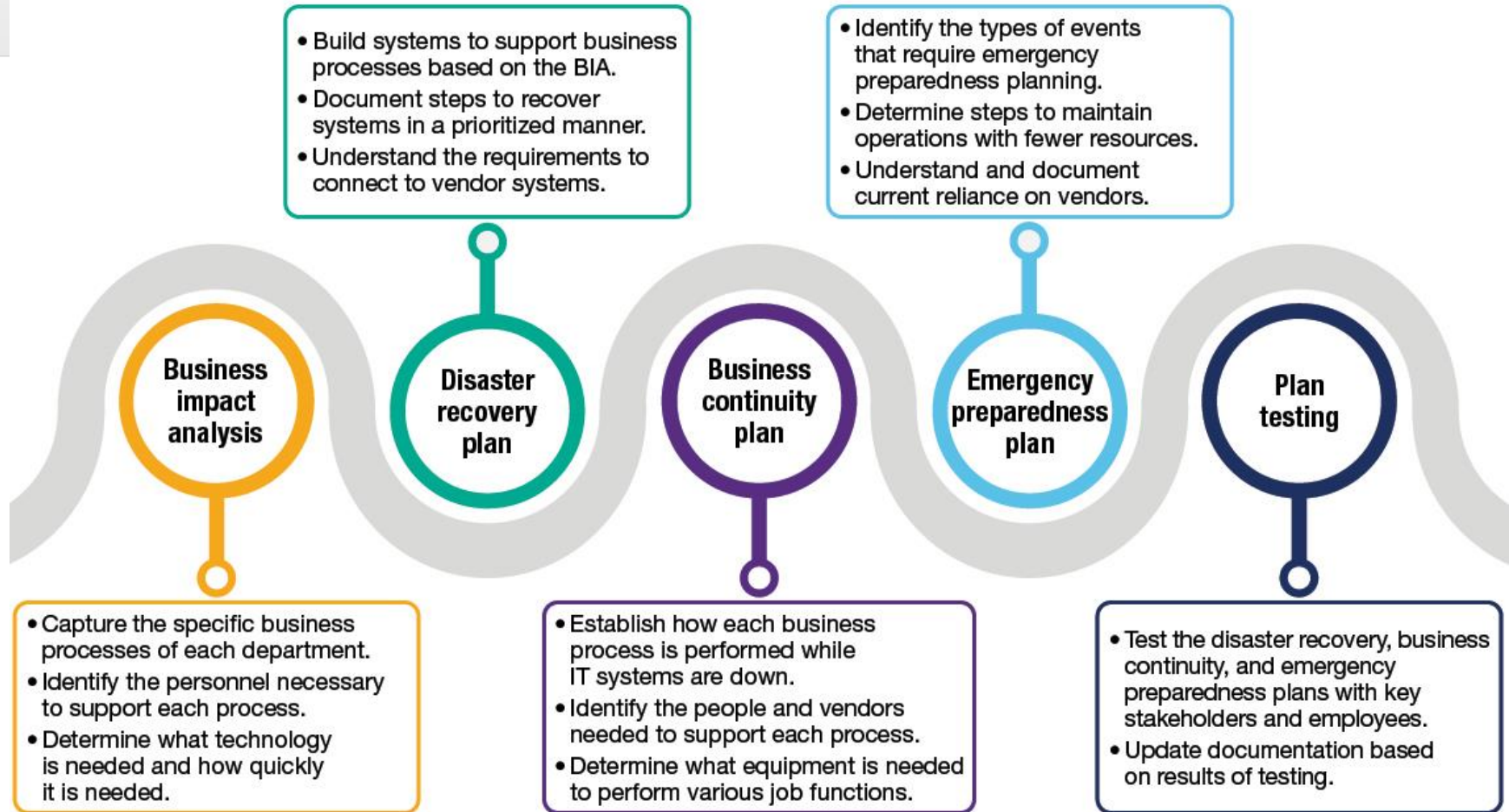


- I. Information Security
- II. Information Security Management System
- III. Risk Management
- IV. Incident Management
- V. Business Continuity & Incident Management**
- VI. Information Security Measurement
- VII. Further Information Security processes
- VIII. Literature

V. Business Continuity Management



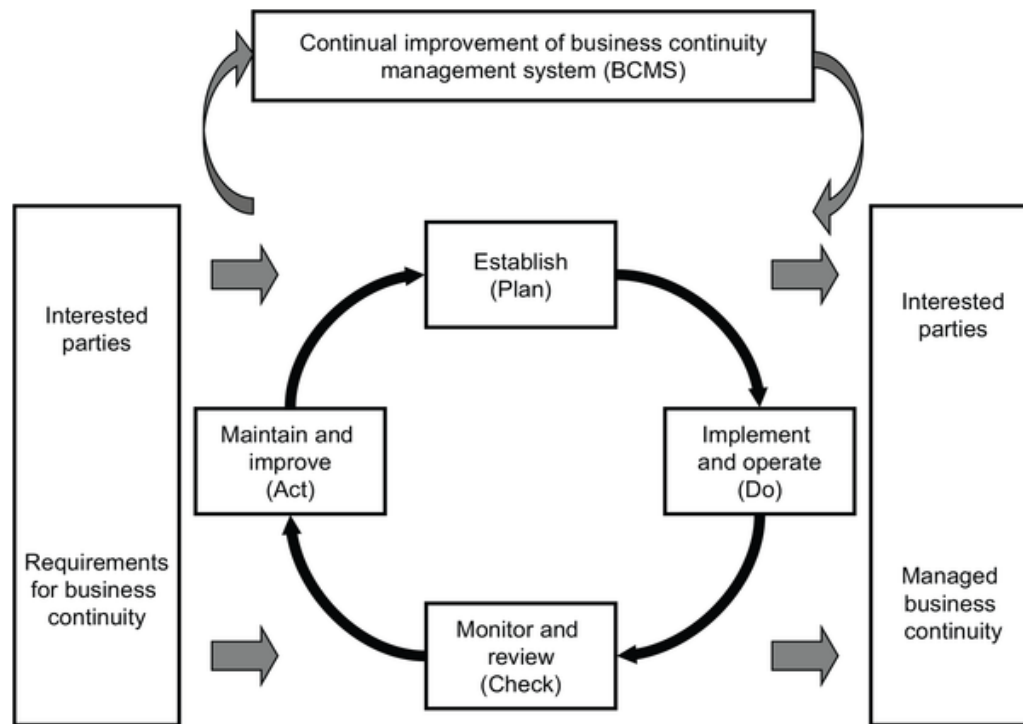
V. Business Continuity Management



V. Business Continuity Management

ISO 22301:2019 - specifies requirements to **plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system** to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise

BCM process

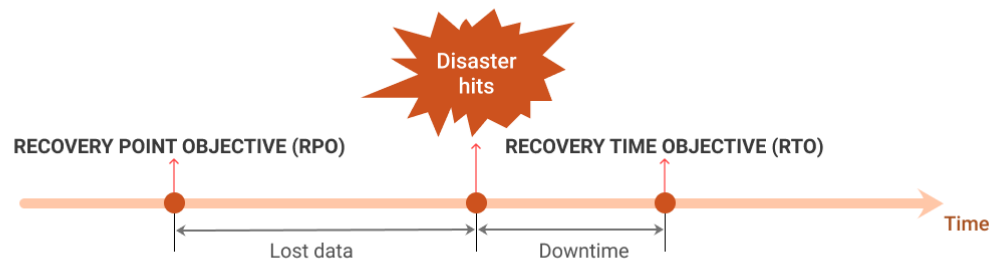


V. Business Continuity Management

Recovery Point Objective (RPO) describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance".

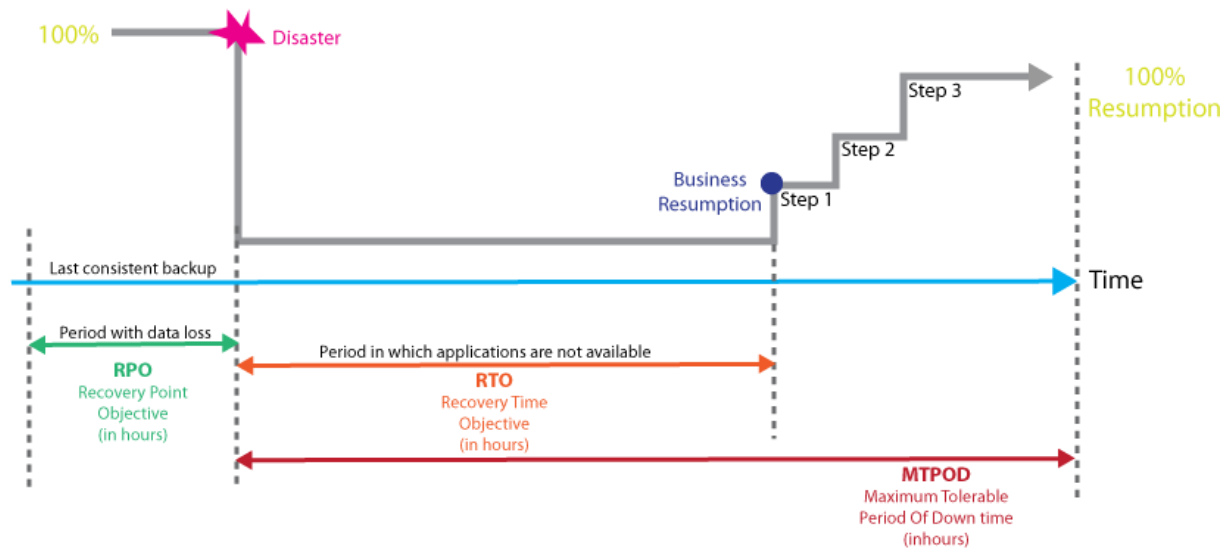
The **Recovery Time Objective (RTO)** is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity. In other words, the RTO is the answer to the question: "How much time did it take to recover after notification of business process disruption?"

RPO and RTO explained



V. Business Continuity Management

Defining RTO, RPO and MTPOD



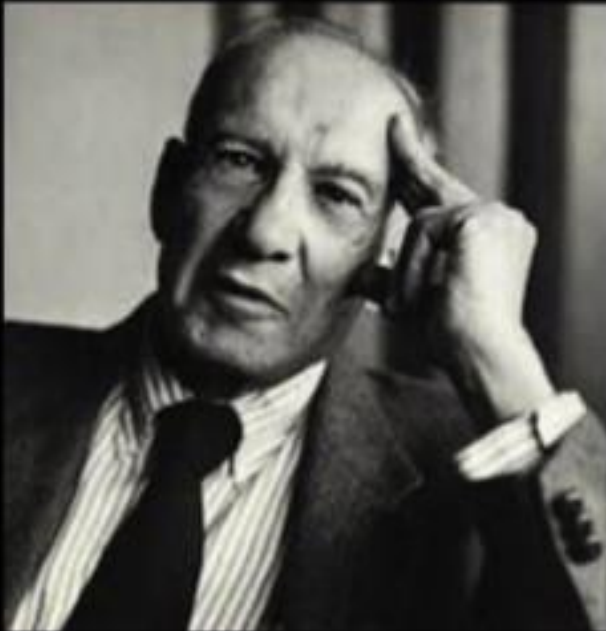
<p>RPO is the maximum acceptable level of data loss following an unplanned "event",</p>	<p>RTO is defined as the length of time that a business process could be unavailable before the business unit's operations are significantly impaired.</p>	<p>MTPOD is defined as the "duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed."</p>
--	---	--

MTPOD can be calculated on the following factors :

- > The maximum time period after the start of a disruption within which each activity needs to be resumed
- > The maximum level at which each activity needs to be performed after resumption
- > The length of time within which normal level of operation need to be resumed

- I. Information Security
- II. Information Security Management System
- III. Risk Management
- IV. Incident Management
- V. Business Continuity Management
- VI. Information Security Measurement**
- VII. Further Information Security processes
- VIII. Literature

Information Security Measurement



**“If you can’t
measure it,
you can’t
manage it”**

Peter Drucker

Key Performance Indicator (KPI)



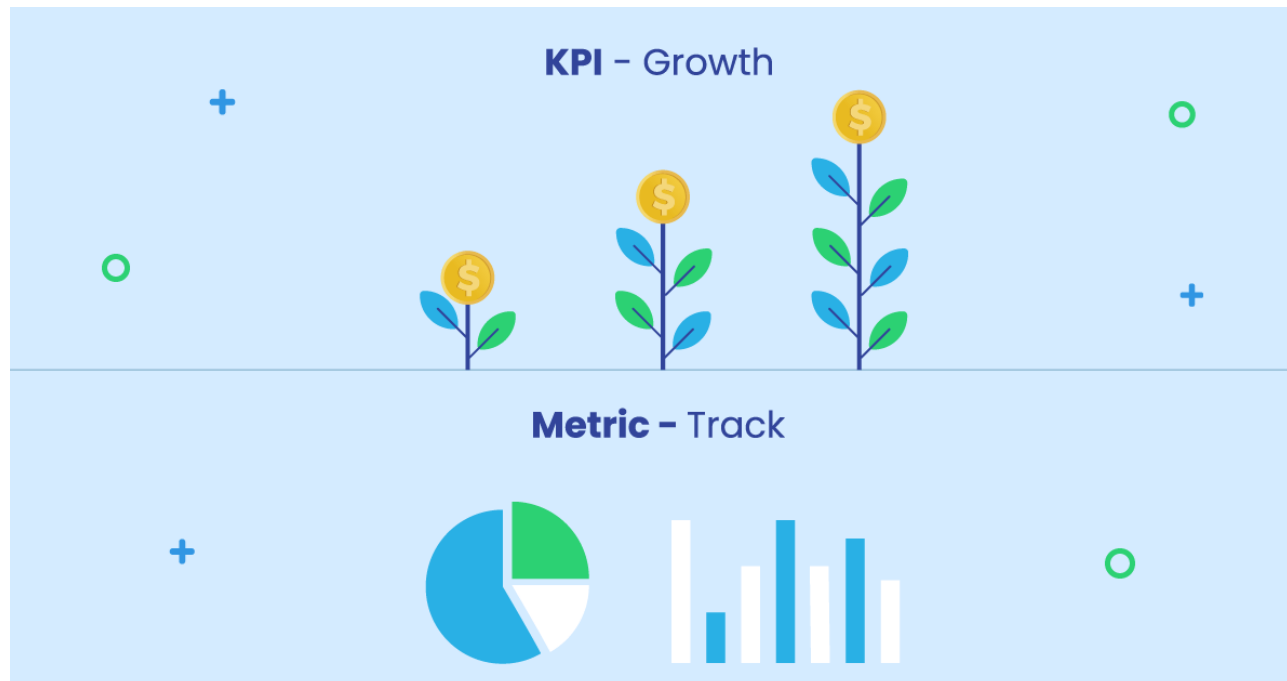
KEY PERFORMANCE INDICATOR



VI. Information Security Measurement

Difference between a metric and an indicator

- A **key performance indicator** is used to measure performance and success.
- A **metric** is nothing more than a number within a KPI that helps track performance and progress.



VI. Information Security Measurement



VI. Information Security Measurement



- I. Information Security
- II. Information Security Management System
- III. Risk Management
- IV. Incident Management
- V. Business Continuity Management
- VI. Information Security Measurement
- VII. Further Information Security processes**
- VIII. Literature

VII. Further Information Security processes

- Identity and Access Management
- Information Classification Management
- Protection Requirements
- Password Management
- Supply Chain Management
- Software Asset Management
- Patch and Vulnerability Management
- Audits and Penetration Testing
- Logging and Monitoring
- Cryptography
- Awareness
- Application Security
- Cloud Security
- Physical Security
- Endpoint Security

- I. Information Security
- II. Information Security Management System
- III. Risk Management
- IV. Incident Management
- V. Business Continuity Management
- VI. Information Security Measurement
- VII. Further Information Security processes
- VIII. Literature**

- Management of Information Security, M. E. Whitman, H. J. Mattord
- Guide to Disaster Recovery, M. Erbschilde
- Guide to Network Defense and Countermeasures, G. Holden
- Real Digital Forensics: Computer Security and Incident Response, 1/e; Keith J. Jones, Richard Bejtlich, Curtis W. Rose
- Computer Security: Art and Science, Matt Bishop (ISBN: 0-201-44099-7), Addison-Wesley 2003
- Security in Computing, 2nd Edition, Charles P. Pfleeger, Prentice Hall

Thank you for your attention



Chair of Mobile Business & Multilateral Security

Michael Schmid

Goethe University Frankfurt

E-Mail: michael.schmid@m-chair.de

WWW: www.m-chair.de

I. Introduction Security Management

Security Management, what is Security Management?

To understand the main purpose of Security Management we need to look at both Security and Management in their individual roles and current descriptive meanings in the industries of today.

Security

Security of today is very different from what it was perceived at the turn of the 20th Century. Security is constantly evolving to meet the requirement of **tackling the ever evolving 'Threat' and the needs of the organisation.** It is not only for the purposes of the commercial industry as it also interacts with the public on a daily basis.

I. Introduction Security Management

Management

The word Manage comes from the Italian maneggiare [maned'dZa:re] (to handle, especially tools), which derives from the Latin word manus (hand). The French word ménagement [menazmã] influenced the development in meaning of the English word management in the 17th and 18th centuries.

Management is a word commonly used to describe a position of responsibility in the Business, Political, Cultural or Social industries.

There are various definitions of management, yet the industry standard is simply defined as a **process of getting the task completed efficiently** with and through other people in accordance with the organisations policies and objectives.

I. Introduction Security Management

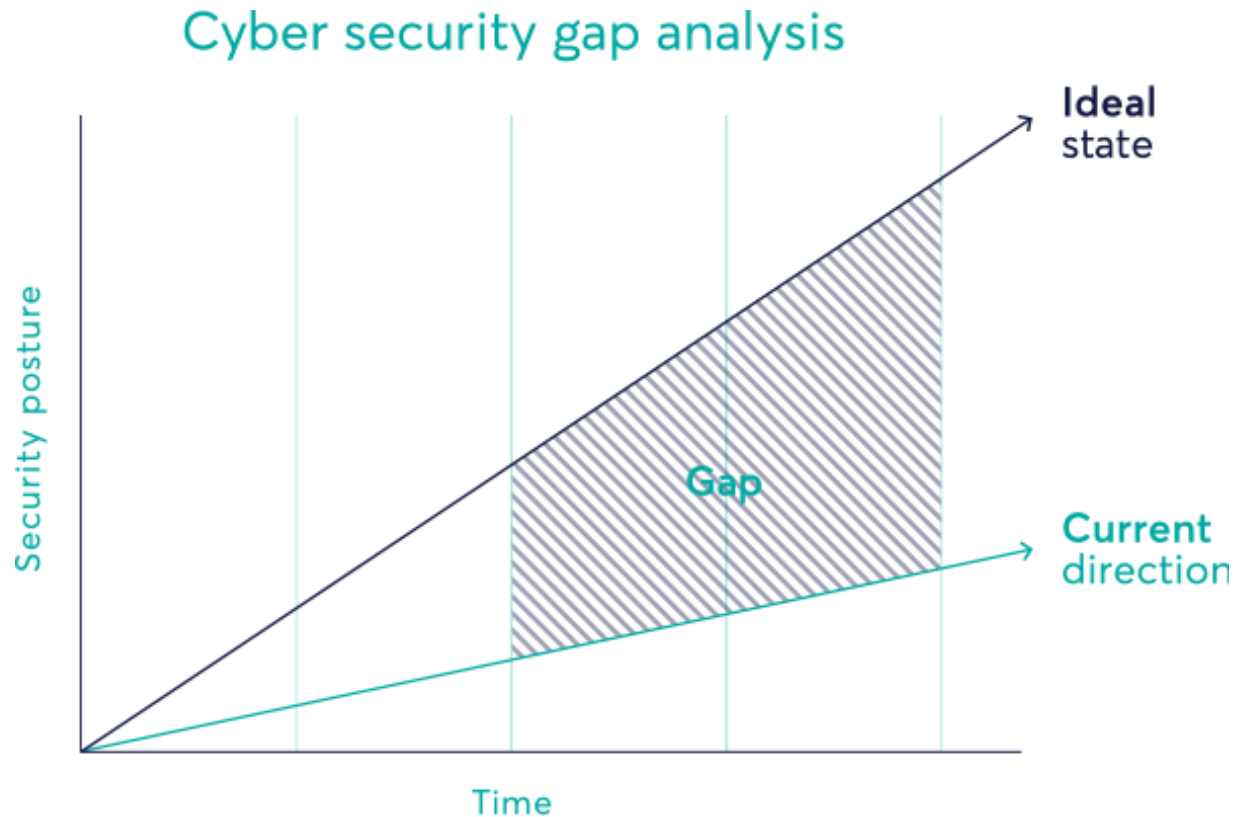
What is the main purpose of Security Management?

One of the main tasks to be completed upon appointment is to carry out a **full risk assessment of the threat the organisation** is exposed to. This includes the following:

- Internal practices & procedures – This includes examining the organisations activities from recruitment to how the organisations records are kept in compliance with the new GDPR regulations, as well as how it conducts its day to day business.
- Physical risks to premises – Conducted by assessing the plans for the premises and evaluating the points of entry, not just the normal entrance points but those subject to risk to be entered through illegally i.e. a ground floor window.
- External risks – There are wide ranging factors involved when assessing the external risks. The location, building, current criminal activities within the area as well as the surrounding environment and accessibility of the location.

II. Information Security Management System

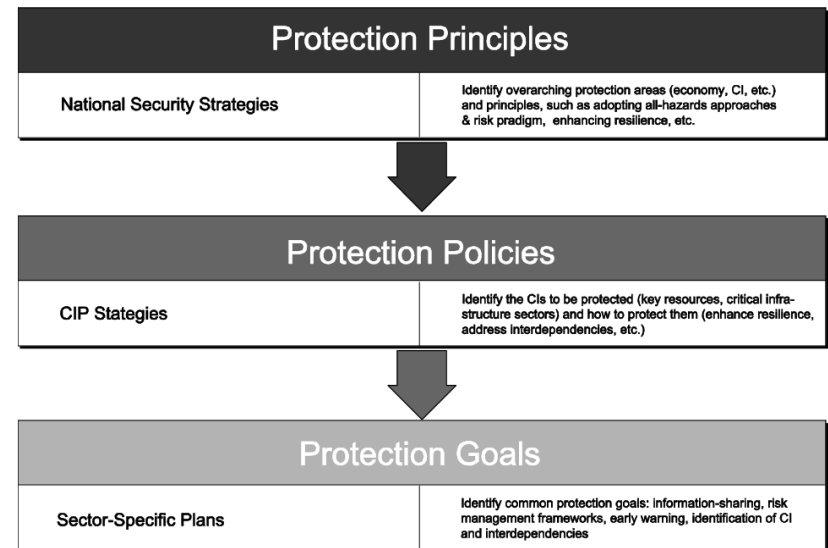
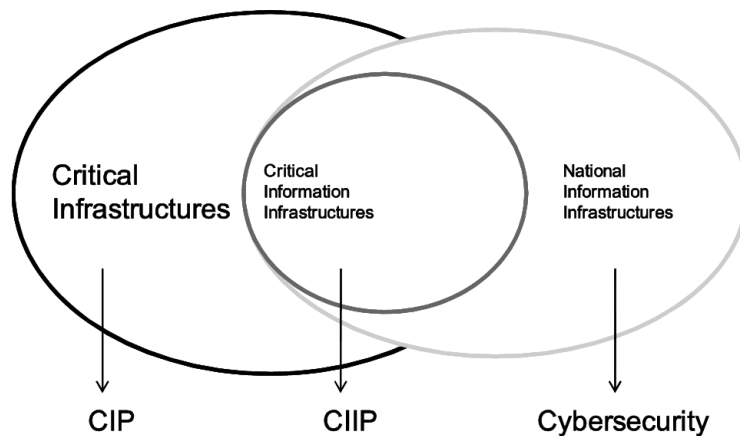
A **gap analysis** helps determine the steps required to reach your ideal cyber security posture.



II. Information Security Management System

Regulatory requirements in Germany that enforce security management

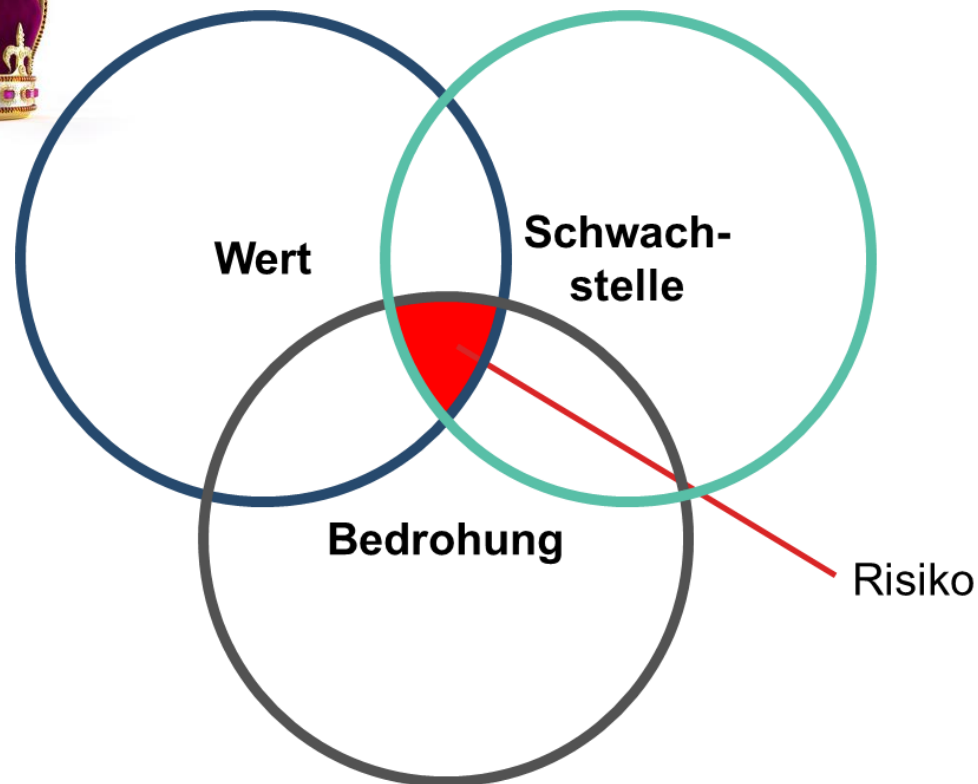
- **Critical Information Infrastructures Protection (CI(I)P)** discover key issues, developments, and trends in order to make recommendations about strategy making in the field of CIIP.

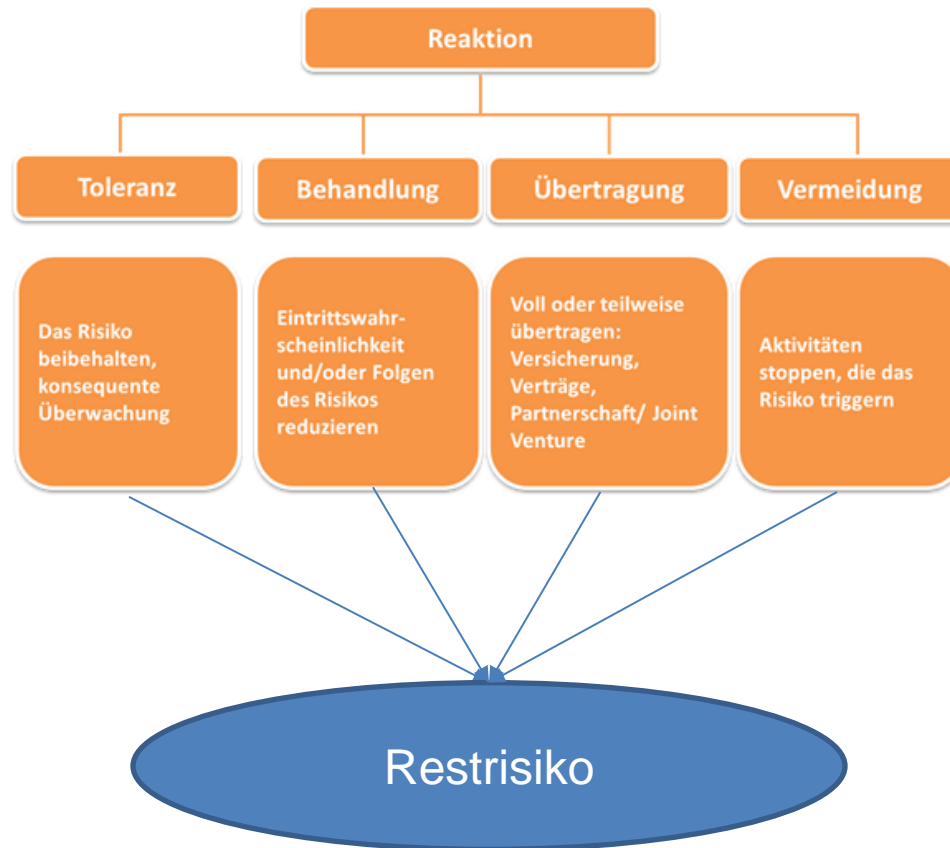


German IT Security Law "1.0"

- Amending act, no codification of IT security
- Entered into force on 25th July 2015
- Amended various existing laws:
 - Act on the Federal Office for Information Security (BSIG)
 - Atomic Energy Act (EnWG)
 - Telemedia Act (TMG)
 - Telecommunications Act (TKG)
 - Act on the Federal Criminal Police Office (BKAG)
- Mostly referring on the protection of Critical Infrastructures, but also including a general extension of power of the BSI according to Sec. 7 BSIG (warnings), Sec. 7a BSIG (examination of IT security)
- Concretization of the scope of application through the BSI-Kritis Regulation, referring to Critical Infrastructures which are defined by certain thresholds in numbers: Energy, Health, ICT, Transport&Traffic, Media, Water, Finance&Insurance, Food, State&Administration

Asset-
inventory





V. Business Continuity Management

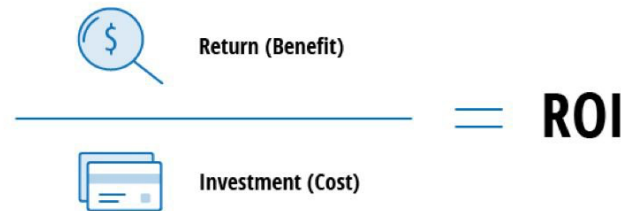
Business Impact Analysis (BIA)

A BIA is a process that allows us to identify critical business functions and predict the consequences a disruption of one of those functions would have. It also allows us to gather information needed to develop recovery strategies and limit the potential loss.

Completing a BIA will assess the risks of a disaster on the organization. It will allow for each department within your organization to explain and discuss how an unexpected event would affect their business function. This will then help your organization prioritize specific functions through the use of Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).

Defining ROI and ROSI

Return On Investment (ROI) is a profitability ratio for a specific investment. It helps you determine whether you should make a purchase or skip it, or how a particular investment has performed to date. The simplest way to calculate ROI is to quantify some kind of “return” or “benefit” and divide it by the “investment” or “cost”:

$$\frac{\text{Return (Benefit)}}{\text{Investment (Cost)}} = \text{ROI}$$


VI. Information Security Measurement

Defining ROI and ROSI

Return On Security Investment (ROSI) means that by looking at all costs (including those caused by damage from an attack) it can be shown whether and when an investment in information security measures leads to a return on investment or not.

$$\begin{array}{l}
 \text{ROSI (\%)} \\
 \text{Quantitative Risk} \\
 \text{Assessment Formula}
 \end{array}
 =
 \frac{\text{ALE * Mitigation Ratio - Cost of Solution}}{\text{Cost of Solution}}$$

Annualized Loss Expectancy (ALE) =
Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO)

$$\text{ALE} = \text{SLE} * \text{ARO}$$