Mobile Business II SS 22

Guest Lecture 2

Information Security Governance, Risk and Compliance at a glance and in motion

28th June 2022, Frankfurt

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

Speaker

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

- since 2012 deputy CISO @Hubert Burda Media Holding KG
- since 2017 PhD student @m-chair
- since 2017 founder and board member of AUDEG - Deutsche Auditoren eG
- University Lecturer & Scientific Reviewer
- > 15 years experience in the field of IT / Information Security
- areas of focus: ISMS, IT Compliance & Governance and Risk Management
- active participation in (inter)national committees: UPKRITIS, ISACA, GI & RMA

Agenda

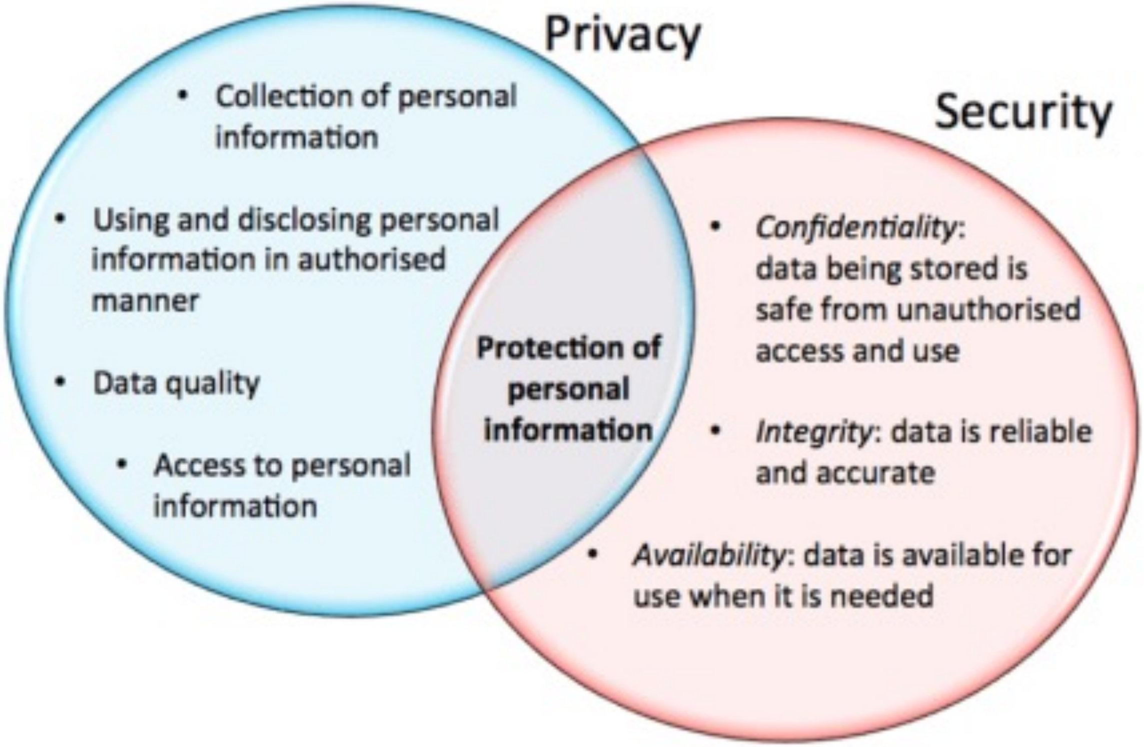
I. Introduction Information Security
II. Introduction Governance, Risk and Compliance (GRC)
III. Information Security Governance
IV. Information Security Risk Management
V. Information Security Compliance
VI. Hands-on Approach to the Implementation of Information Security GRC

Agenda

I. Introduction Information Security
II. Introduction Governance, Risk and Compliance (GRC)
III. Information Security Governance
IV. Information Security Risk Management
V. Information Security Compliance
VI. Hands-on Approach to the Implementation of Information Security GRC

I. Introduction Information Security

Privacy vs. Security



Privacy

- Collection of personal information
- Using and disclosing personal information in authorised manner
- Data quality
- Access to personal information

Protection of personal information

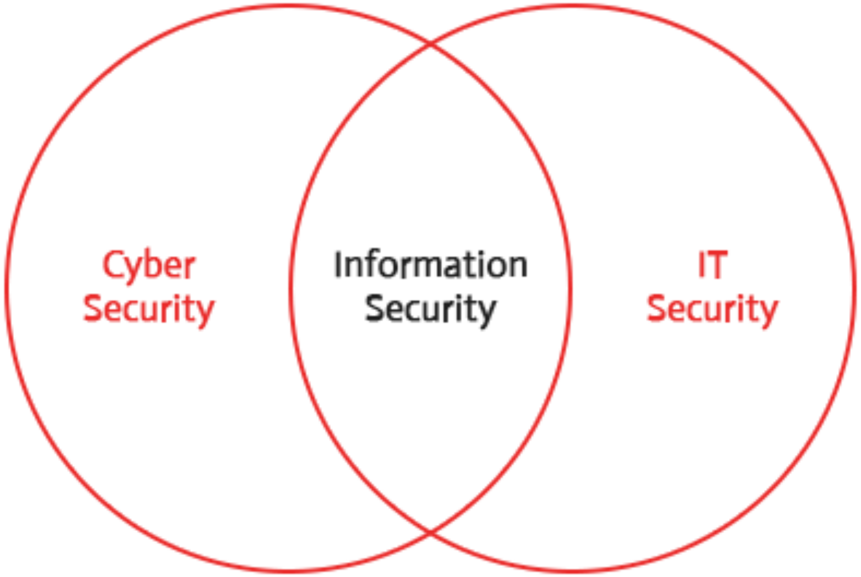
Security

- *Confidentiality*: data being stored is safe from unauthorised access and use
- *Integrity*: data is reliable and accurate
- *Availability*: data is available for use when it is needed

Source: davidfroud.com

I. Introduction Information Security

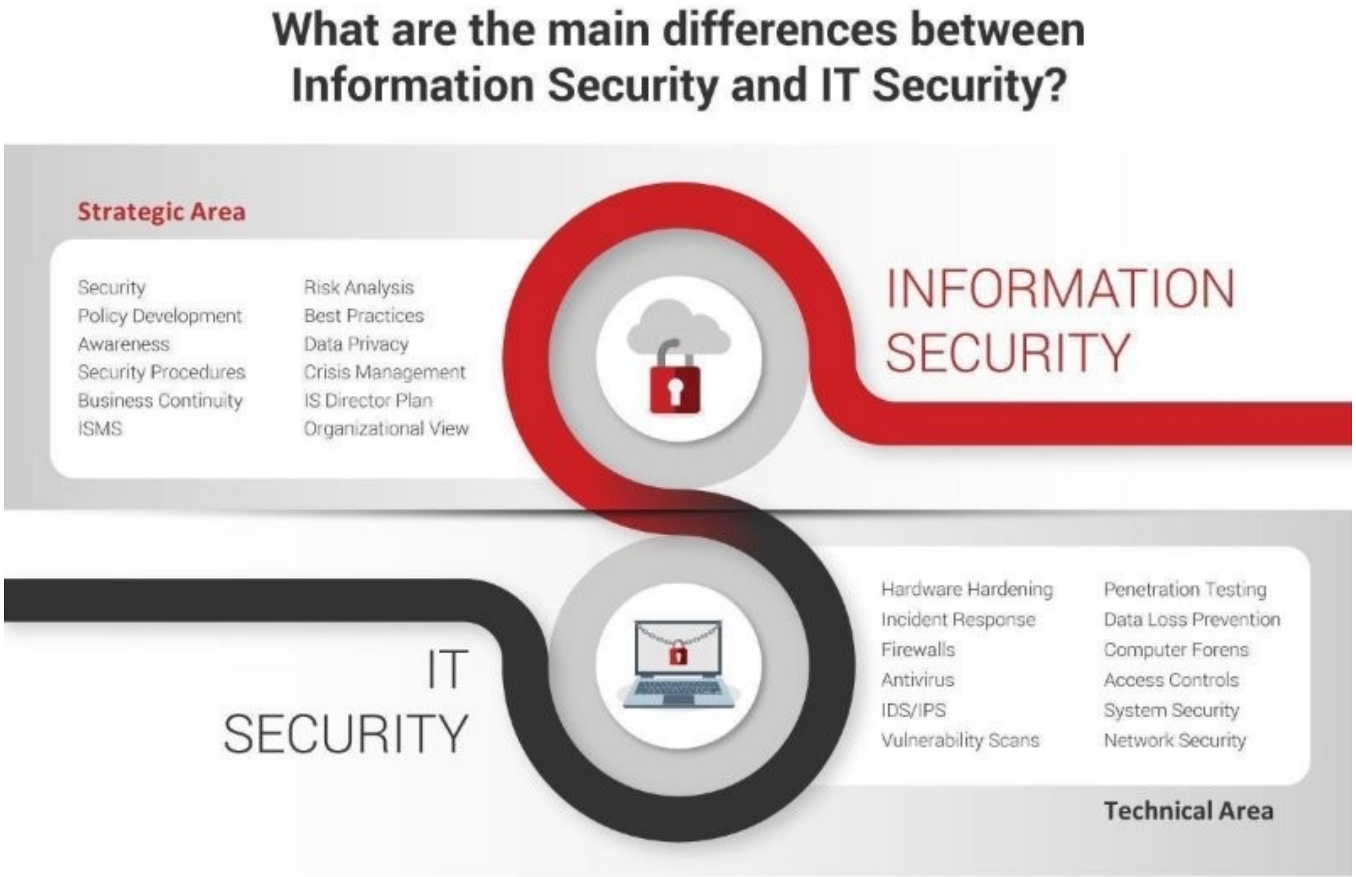
Cyber vs. Information vs. IT Security



Source: businessbeam.com

I. Introduction Information Security

Information vs. IT Security



What are the main differences between Information Security and IT Security?

Strategic Area

Security
Policy Development
Awareness
Security Procedures
Business Continuity
ISMS

Risk Analysis
Best Practices
Data Privacy
Crisis Management
IS Director Plan
Organizational View

Hardware Hardening
Incident Response
Firewalls
Antivirus
IDS/IPS
Vulnerability Scans

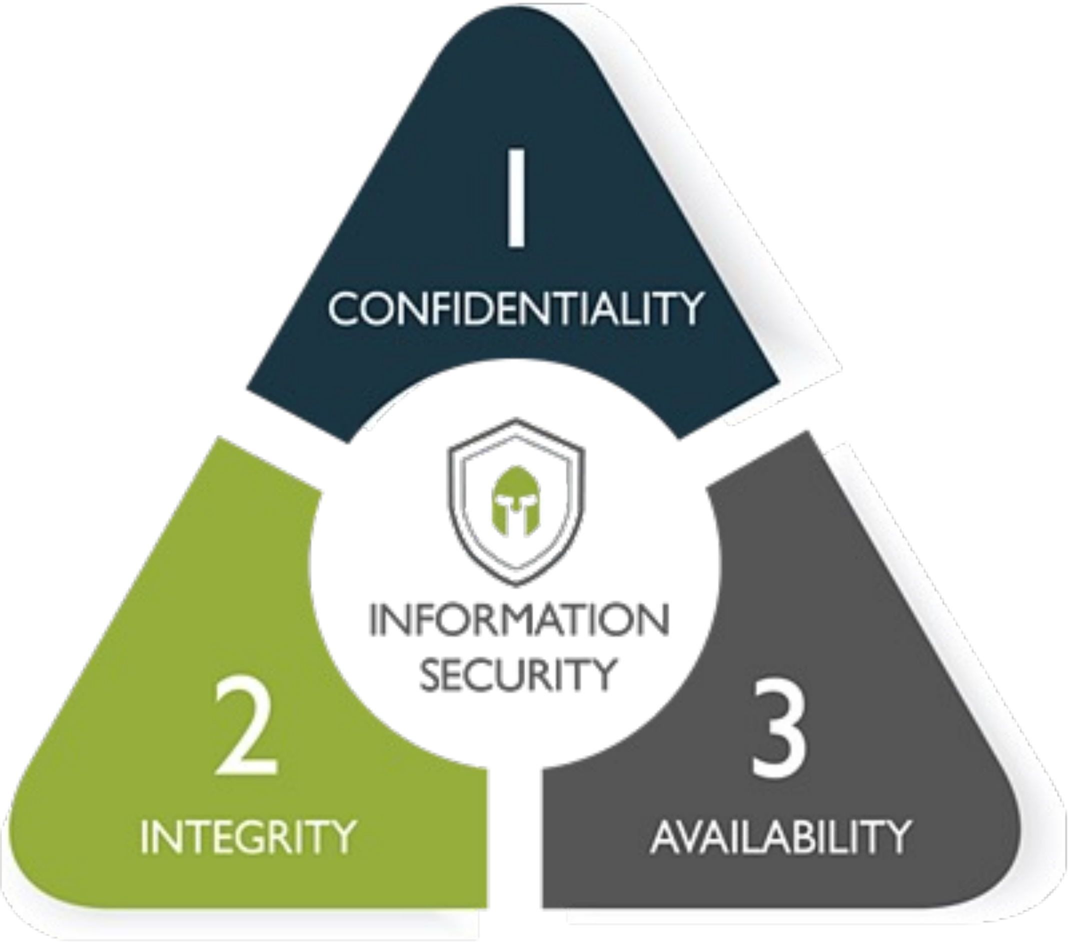
Penetration Testing
Data Loss Prevention
Computer Forens
Access Controls
System Security
Network Security

Technical Area

Source: it-its.org

I. Introduction Information Security

CIA vs. Information security?



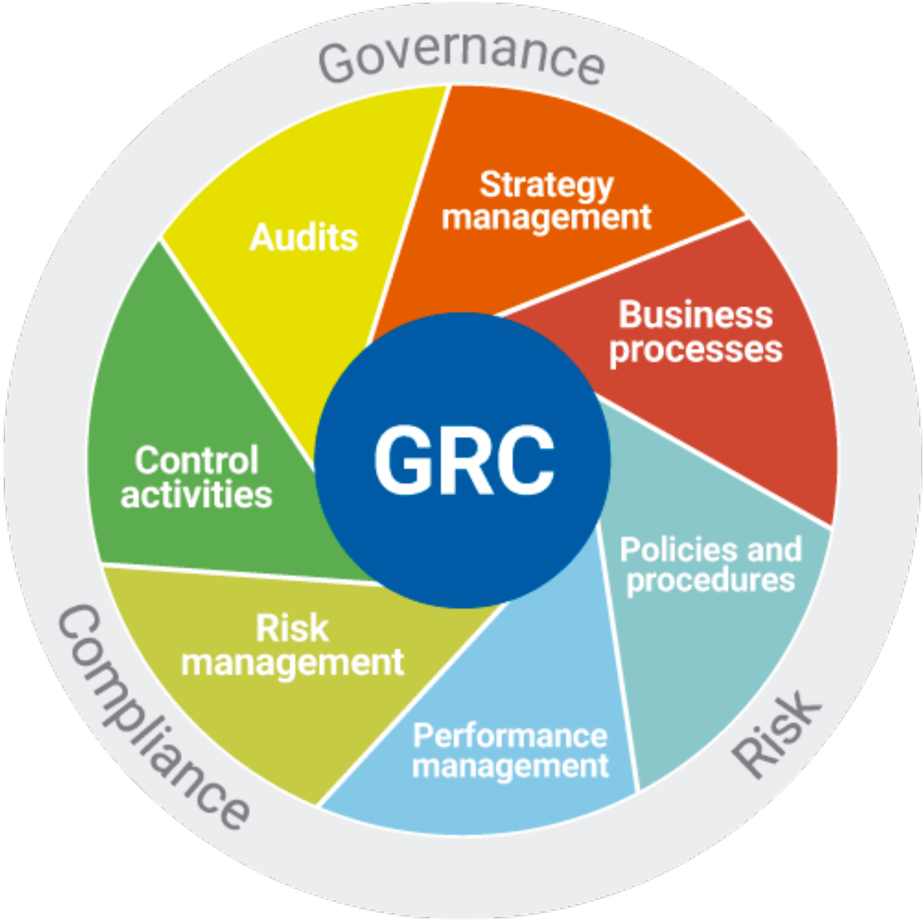
Source: comtact.co.uk

Agenda

I. Introduction Information Security
II. Introduction Governance, Risk and Compliance (GRC)
III. Information Security Governance
IV. Information Security Risk Management
V. Information Security Compliance
VI. Hands-on Approach to the Implementation of Information Security GRC

II. Introduction Governance, Risk and Compliance (GRC)

Governance, **R**isk and **C**ompliance (GRC)



Source: softexpert.com

II. Introduction Governance, Risk and Compliance (GRC)

Three important levels of action for the company
Governance, risk and compliance (GRC) describes the handling of information worthy of protection and can be used as an umbrella term for the three most important levels of action of a company.

Governance - governance means leadership and defines the management of a company by means of guidelines, such as the definition of corporate goals, the methodology applied to achieve them, or the planning of resources to achieve them.

Risk - risk stands for risk management and includes the handling of known and unknown risks on the basis of a previously defined risk analysis and the management of the risks. In this way, companies deal with risks at an early stage or strategies are developed for risk minimization and crisis management in the event of risk occurrence. Risk management is primarily based on internal policies. The company protects itself and has a vested interest in implementing these policies.

Compliance - Adherence to internal and external standards for the provision and processing of information is the third key area of GRC. Compliance includes, among other things, the specifications from standardization efforts and the access regulations for data as well as the legal framework for its use.

II. Introduction Governance, Risk and Compliance (GRC)

The general objective of GRC thus comprises three points:

1. Identifying risks and taking measures to manage them

2. ensuring that the standards and laws resulting from step one are complied with

3. comparing processes on the basis of best practice approaches

Agenda

I. Introduction Information Security
II. Introduction Governance, Risk and Compliance (GRC)
III. Information Security Governance
IV. Information Security Risk Management
V. Information Security Compliance
VI. Hands-on Approach to the Implementation of Information Security GRC

III. Information Security Governance

Source: linkedin.com

]

III. Information Security Governance

Governance is the set of broad principles and values that guide the way you manage your organization. It is about the vision, mission and values of your business. Corporate governance is the soul of your business; it keeps everyone on track and helps you reach your goals.

In this piece we take a look at **information security governance**: the principles and vision that guide the process by which you create an effective information security system.

Information security governance plays an important role in the **business** world today, because it allows you to show potential business partners that you have an actual governance structure and process that guides your information security decisions and incident responses. You are running a tight ship, and not leaving anything up to chance.

That quality makes a **business** more attractive to its customer base, and gives you a competitive advantage over rivals that don't apply good governance to their IT security needs.

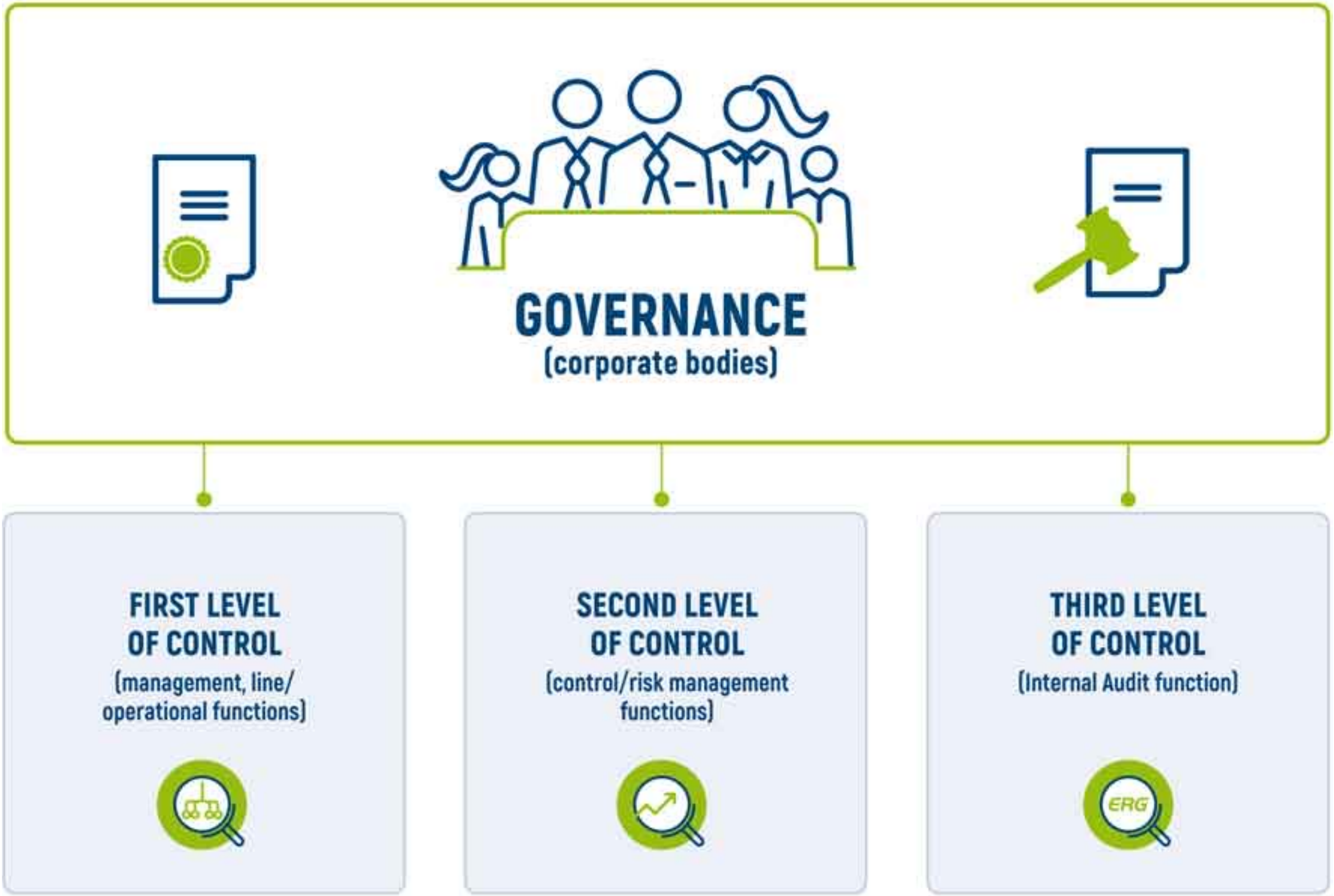
III. Information Security Governance

The Four Goals of Information Security Governance

1. **Provide IT governance** and organizational structure that constantly works to improve data protection. Information security management includes **risk management**, which we can define as the practice of identifying poor practices for handling information that should be avoided, and also having a plan for how to mitigate security incidents and handle new or unexpected information security risks.
2. **Protect business investments** by securing business continuity in case of security breaches or other cybersecurity events. Protect the value of your business and its reputation.
3. **Monitor staff** and define security measures to assure business needs have the highest priority. Compile metrics and make sure your security practices are easy to understand and apply, no matter where in the business they are needed. Remember: any security control is only as good as the metrics you collect from it.
4. Make sure your business stays in **compliance** with regulatory requirements and other standards. Here are some commonly used information security governance frameworks that will help you stay in compliance.

III. Information Security Governance

Three Lines of Defense



GOVERNANCE
(corporate bodies)

FIRST LEVEL OF CONTROL
(management, line/ operational functions)

SECOND LEVEL OF CONTROL
(control/risk management functions)

THIRD LEVEL OF CONTROL
(Internal Audit function)

Source: erg.eu

III. Information Security Governance

The role of internal IT audit in information security governance

An internal IT audit can provide a fair and accurate review of governance processes, risk management and internal controls. As the third line of defence for a business, internal audit equips the board with a holistic view of governance structures and how well they are working within the company.

The focus of an IT audit can be based on the organisation's needs and issues, as they are designed to provide assurance on the procedures in place to manage governance structures.

Agenda

I. Introduction Information Security
II. Introduction Governance, Risk and Compliance (GRC)
III. Information Security Governance
IV. Information Security Risk Management
V. Information Security Compliance
VI. Hands-on Approach to the Implementation of Information Security GRC

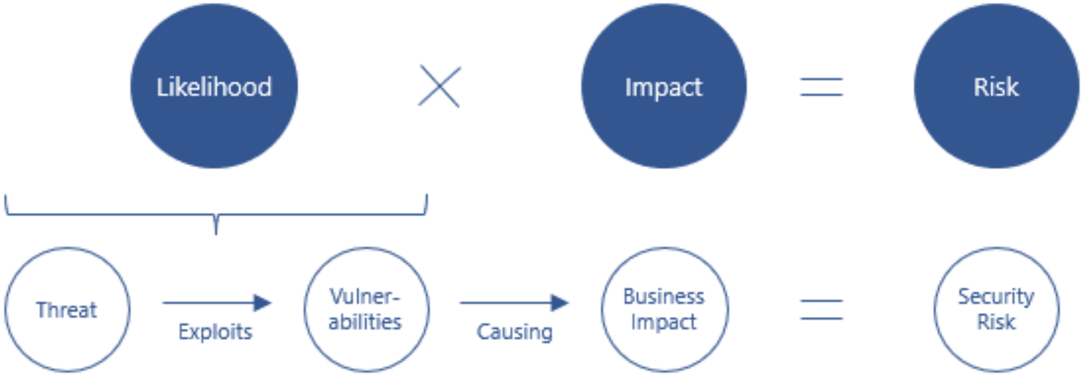
IV. Information Security Risk Management

Source: pngitem.com

IV. Information Security Risk Management

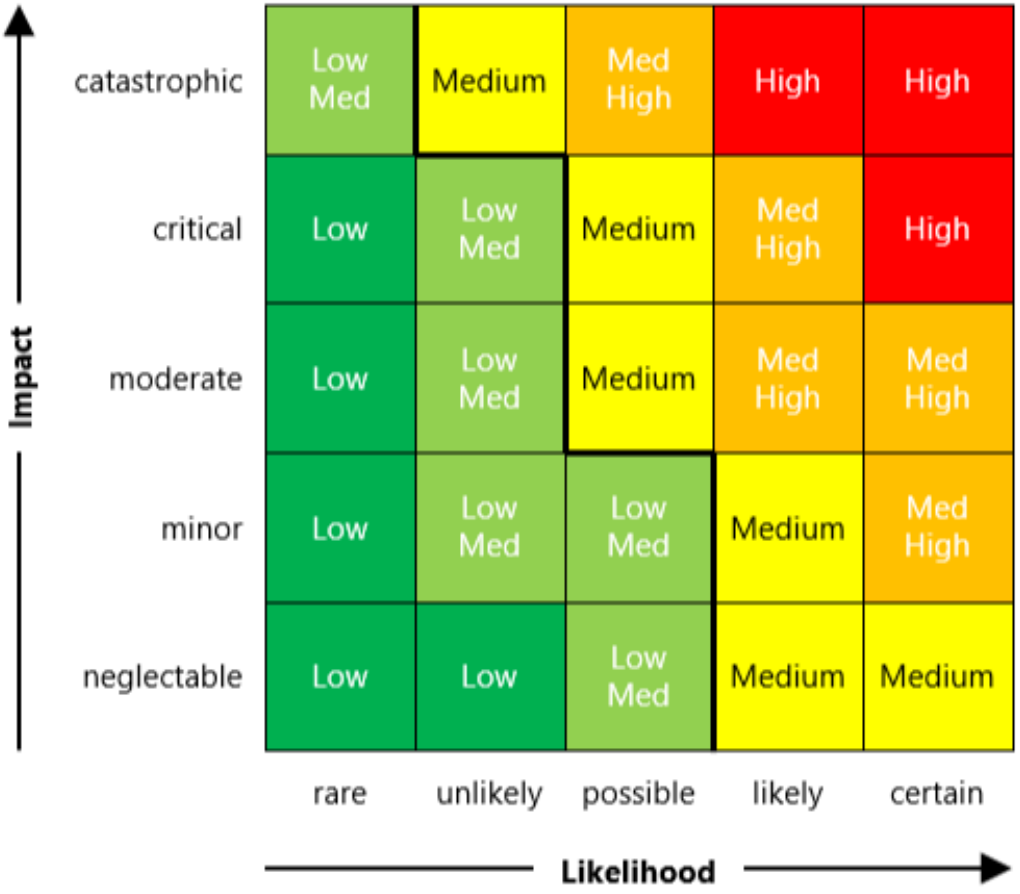
Risk management

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



Source: b-advisory.ch

Risk matrix



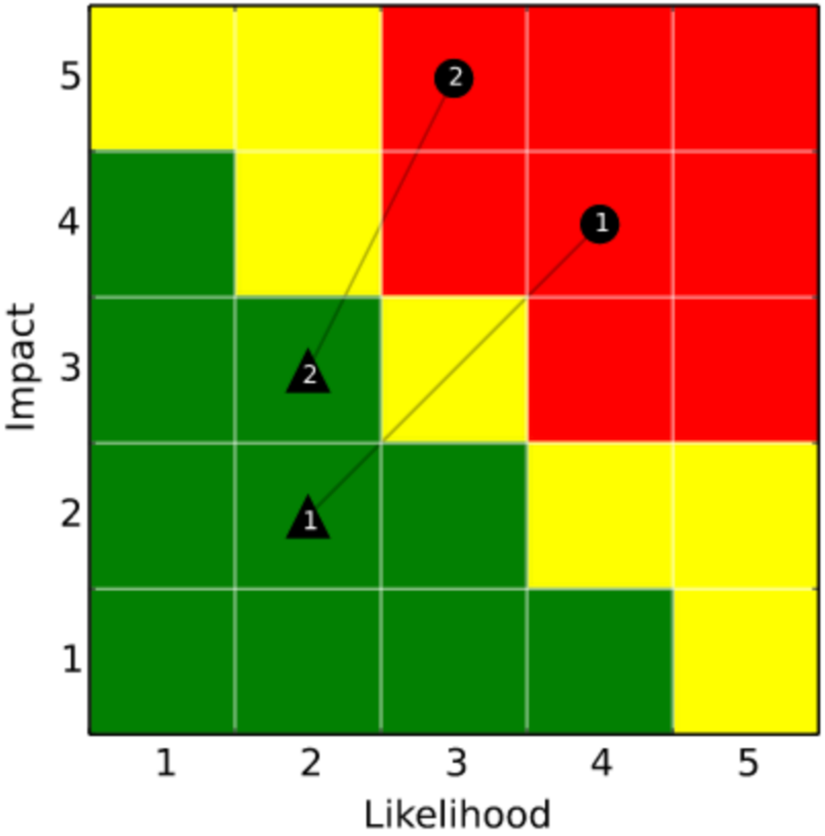
Impact

	rare	unlikely	possible	likely	certain
catastrophic	Low Med	Medium	Med High	High	High
critical	Low	Low Med	Medium	Med High	High
moderate	Low	Low Med	Medium	Med High	Med High
minor	Low	Low Med	Low Med	Medium	Med High
neglectable	Low	Low	Low Med	Medium	Medium

Likelihood

Source: b-advisory.ch

Risk matrix with and without measures

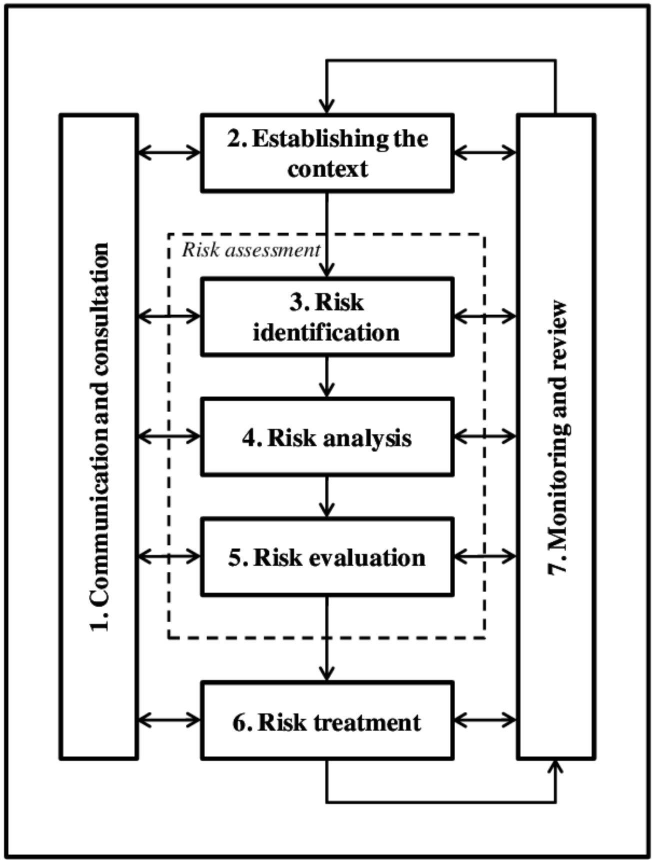


Source: b-advisory.ch

IV. Information Security Risk Management

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

Risk management process

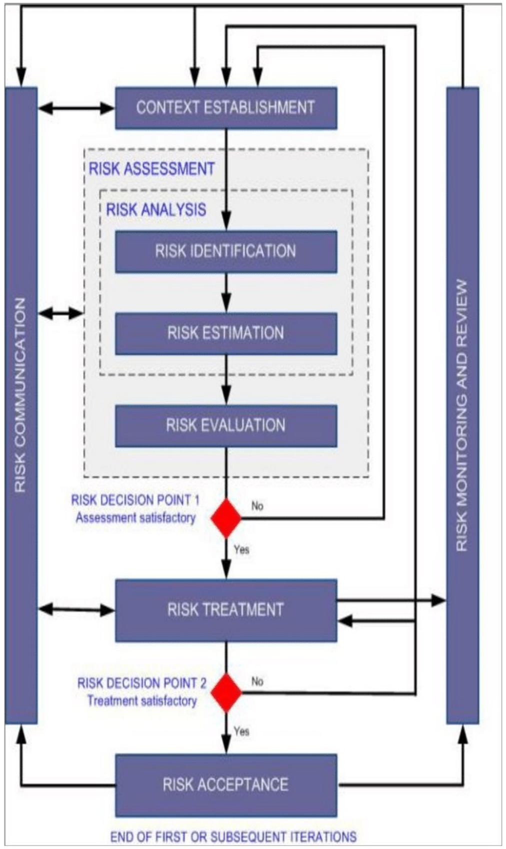


Source: ISO.org

IV. Information Security Risk Management

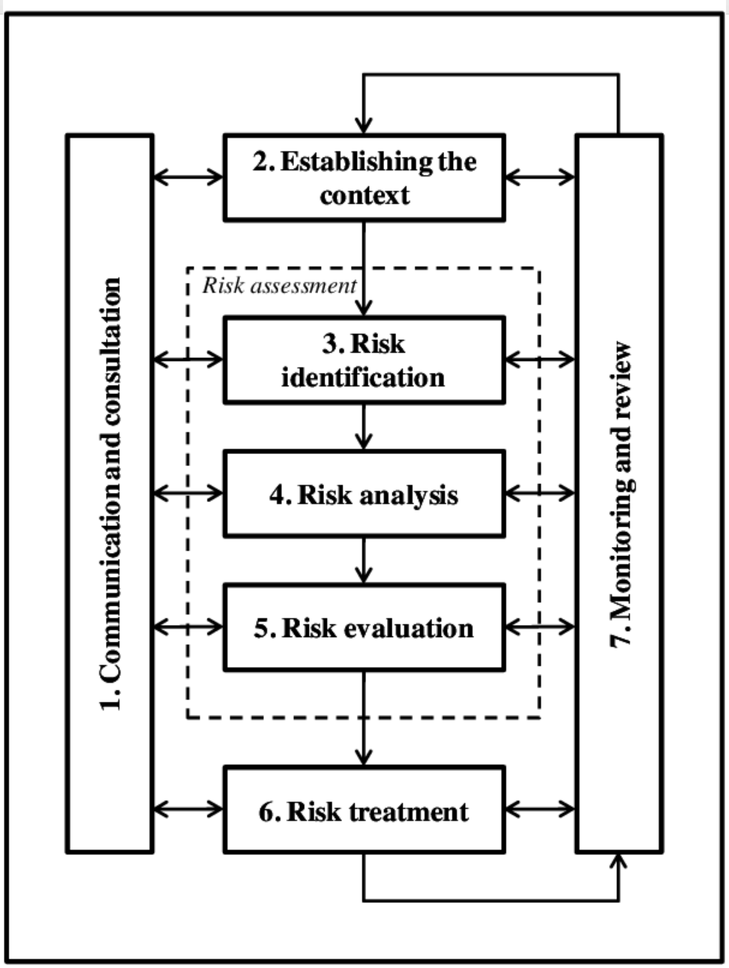
ISO/IEC 27005:2018 - provides guidelines and techniques for managing **information** security risks

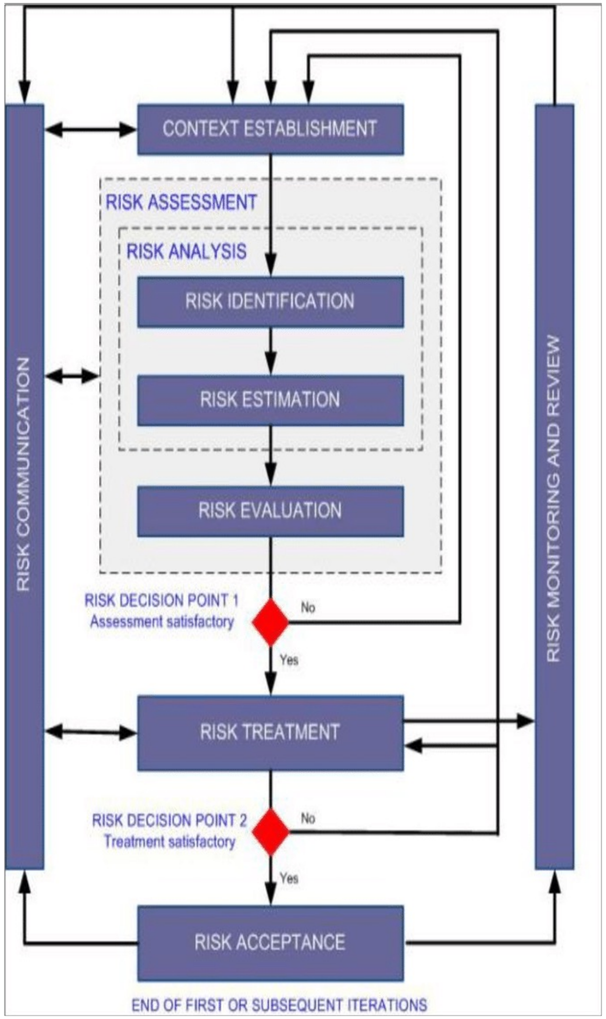
Risk management process



Source: ISO.org

IV. Information Security Risk Management





Source: ISO.org

IV. Information Security Risk Management

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.

Agenda

I. Introduction Information Security
II. Introduction Governance, Risk and Compliance (GRC)
III. Information Security Governance
IV. Information Security Risk Management
V. Information Security Compliance
VI. Hands-on Approach to the Implementation of Information Security GRC

V. Information Security Compliance

External and internal requirements for information security

- Contractual requirements
- External Compliance
  - Basic EU data protection regulation (GDPR)
  - Country-specific telemedia and telecommunications laws
  - NIS Directive (Digital Service Providers: Search Engines, Cloud Services and Marketplaces)
  - Payment Card Industry Data Security Standard (PCI DSS) Processing of credit card data
- Internal compliance (Group guidelines)

V. Information Security Compliance

Relevant standards and best practice with regard to information security

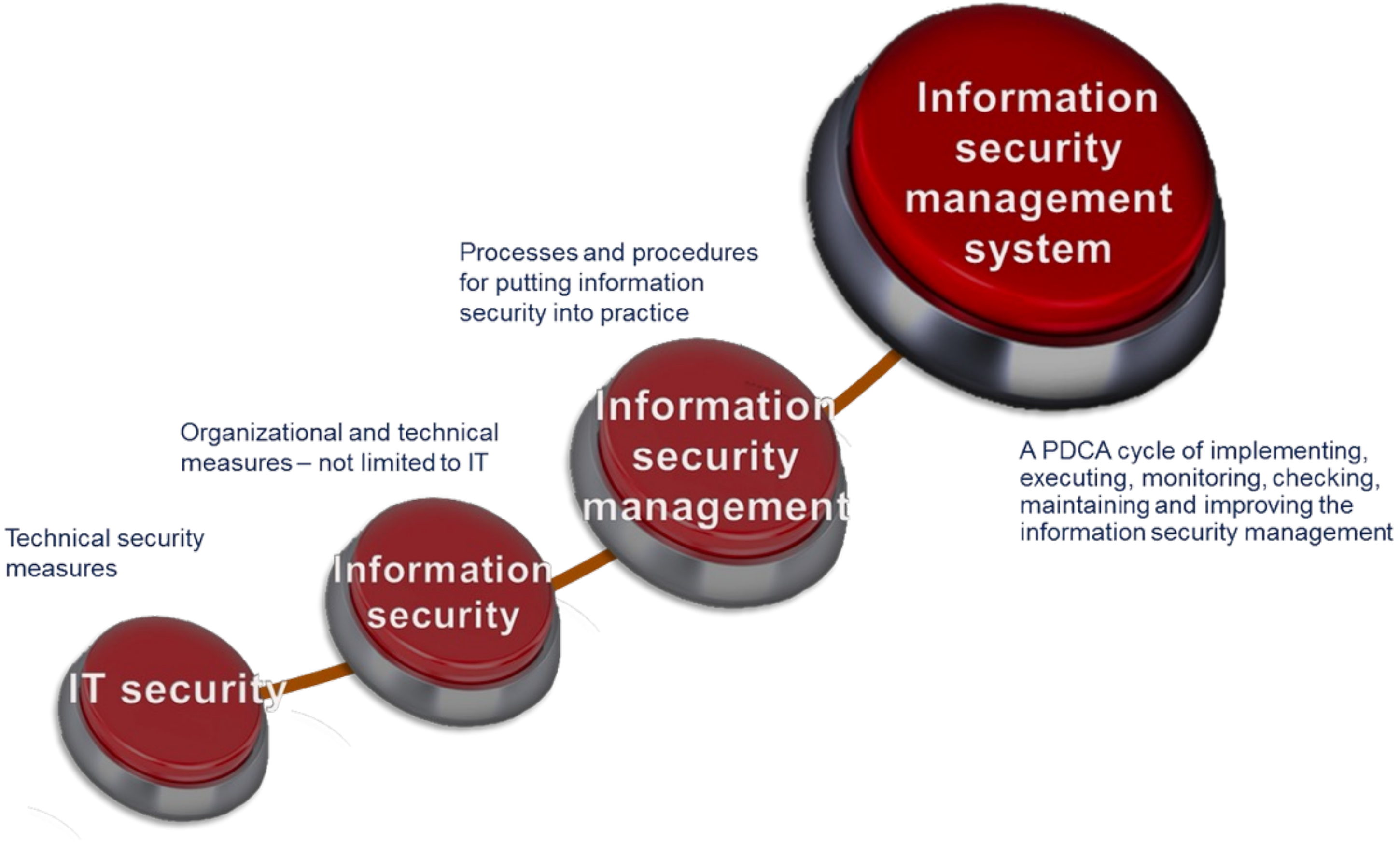
- International Organization for Standardization ISO/IEC 27001 (requirements for the introduction, operation, monitoring, maintenance and improvement of a documented ISMS)
- National Institute for Security and Technology (NIST) publication 800-53
- German Federal Office for Information Security (BSI) (in particular the catalogues of measures for technical infrastructure)
- Health Information Portability and Accountability Act (HIPAA)
- Control Objectives for Information and Related Technology (COBIT) from Information Systems Audit and Control Association (ISACA) (mapping IT processes, maturity model)
- Information Technology Infrastructure Library (ITIL) (for the general mapping of IT service processes)

V. Information Security Compliance

Exemplary Standard

V. Information Security Compliance

From IT security to an Information security management system



Information security management system
Information security management

Processes and procedures for putting information security into practice

Organizational and technical measures – not limited to IT

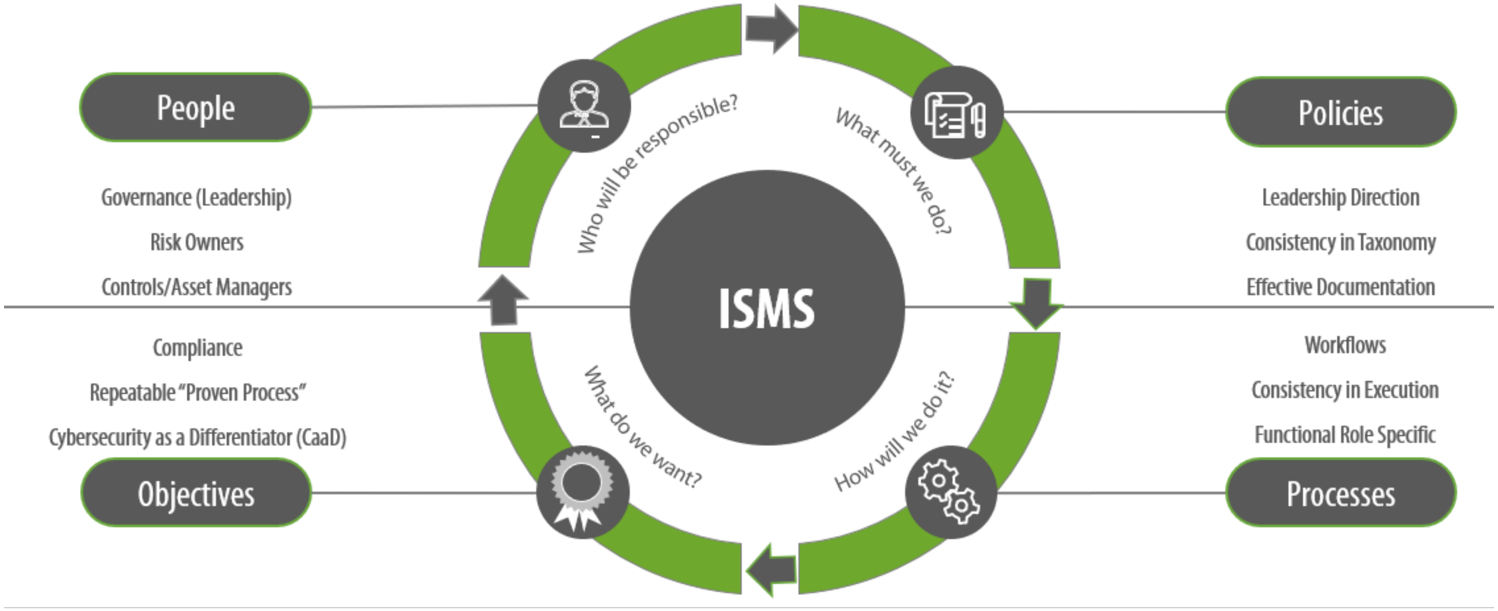
Technical security measures

A PDCA cycle of implementing, executing, monitoring, checking, maintaining and improving the information security management

Source: it-pillars.com

V. Information Security Compliance

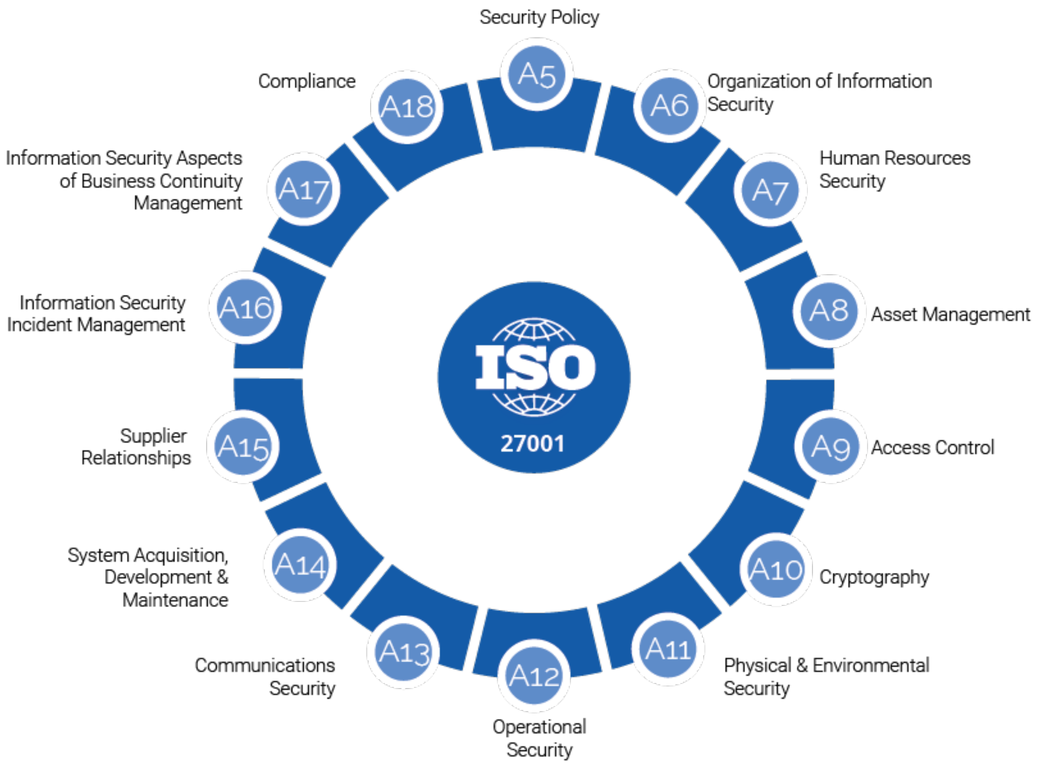
Information **S**ecurity **M**anagement **S**ystem (ISMS)



Source: cyberintsolns.com

V. Information Security Compliance

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

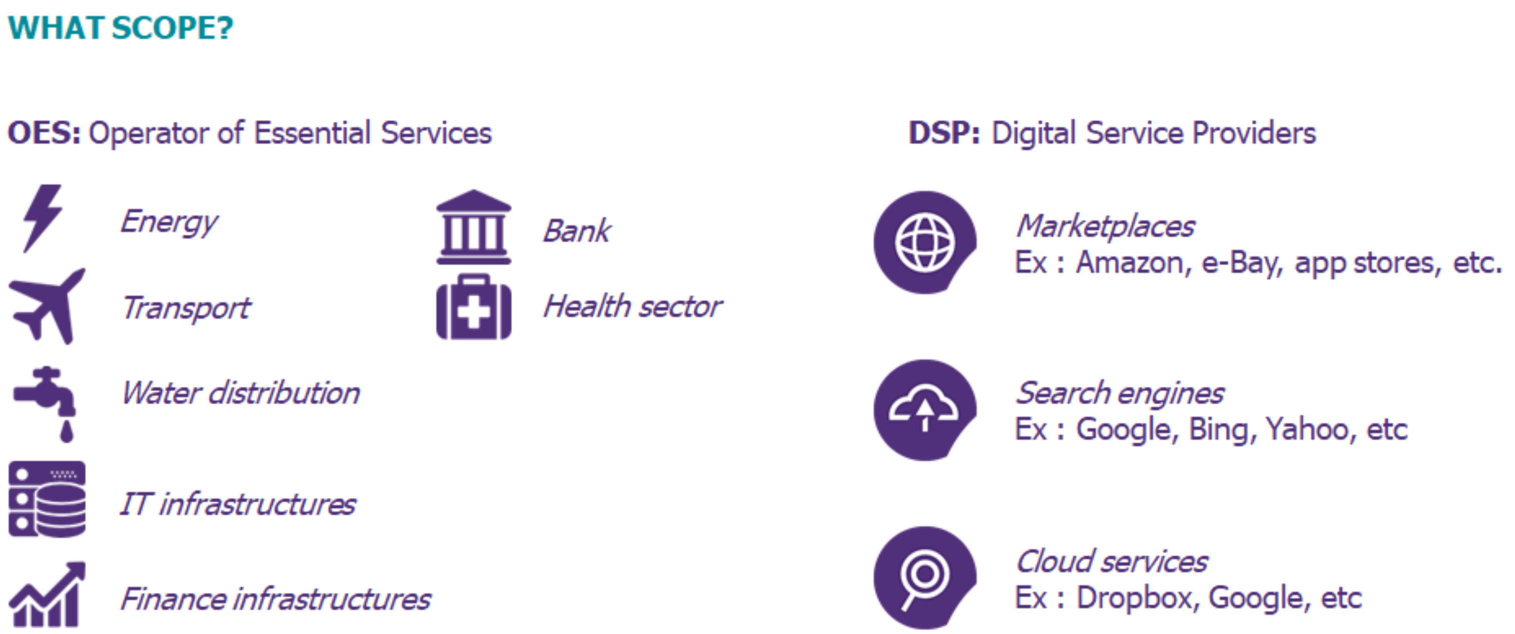

Security Policy
A5
Organization of Information Security
A6
Human Resources Security
A7
Asset Management
A8
Access Control
A9
Cryptography
A10
Physical & Environmental Security
A11
Operational Security
A12
Communications Security
A13
System Acquisition, Development & Maintenance
A14
Supplier Relationships
A15
Information Security Incident Management
A16
Information Security Aspects of Business Continuity Management
A17
Compliance
A18
ISO
27001

Source: caveonix.com

Regulatory Request
(Example for External Compliance)

NIS (Network and Information Security) Directive (EU 2016/1148)

The aim of the directive is to create a **higher level of network and information system security** for Operators of Essential Services (OES) and Digital Service Providers (DSP) throughout the EU.



WHAT SCOPE?

OES: Operator of Essential Services

- *Energy*
- *Transport*
- *Water distribution*
- *IT infrastructures*
- *Finance infrastructures*
- *Bank*
- *Health sector*

DSP: Digital Service Providers

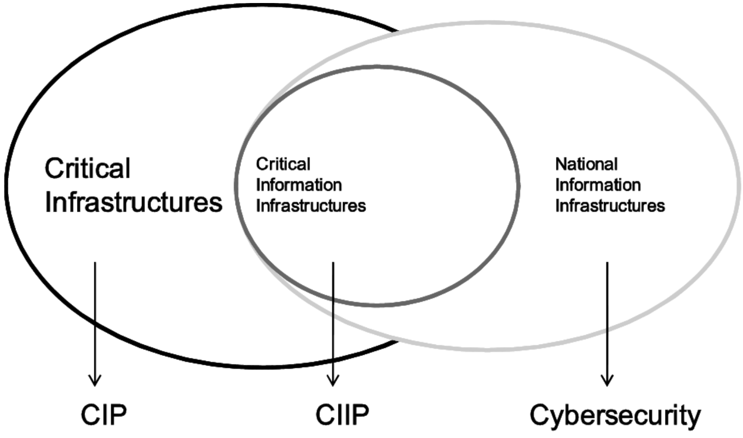
- *Marketplaces*
Ex : Amazon, e-Bay, app stores, etc.
- *Search engines*
Ex : Google, Bing, Yahoo, etc
- *Cloud services*
Ex : Dropbox, Google, etc

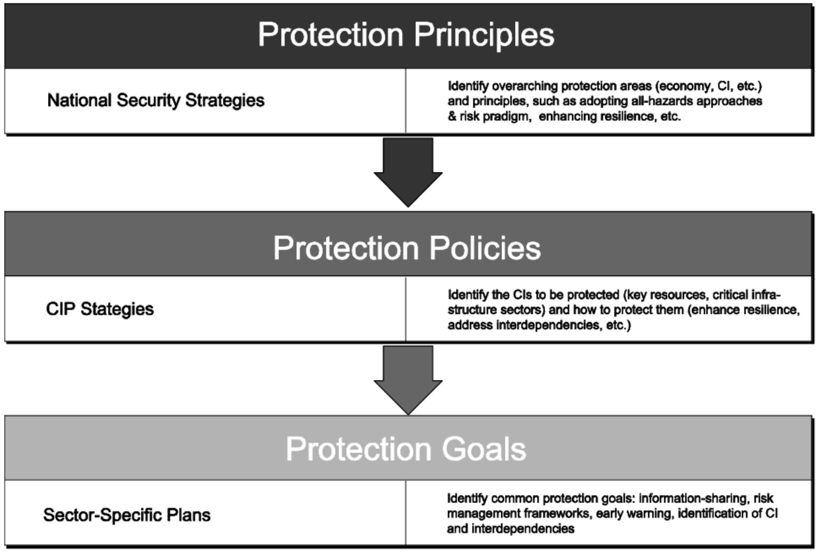
Source: riskinsight-wavestone.com

V. Information Security Compliance

Regulatory requirements in Germany that enforce security management

- **C**ritical **I**nformation **I**nfrastructures **P**rotection (CI(I)P) discover key issues, developments, and trends in order to make recommendations about strategy making in the field of CIIP.


Critical Infrastructures
Critical Information Infrastructures
National Information Infrastructures
CIP
CIIP
Cybersecurity



Protection Principles

National Security Strategies — Identify overarching protection areas (economy, CI, etc.) and principles, such as adopting all-hazards approaches & risk pradigm, enhancing resilience, etc.

Protection Policies

CIP Stategies — Identify the CIs to be protected (key resources, critical infrastructure sectors) and how to protect them (enhance resilience, address interdependencies, etc.)

Protection Goals

Sector-Specific Plans — Identify common protection goals: information-sharing, risk management frameworks, early warning, identification of CI and interdependencies

Source: springer.com

V. Information Security Compliance

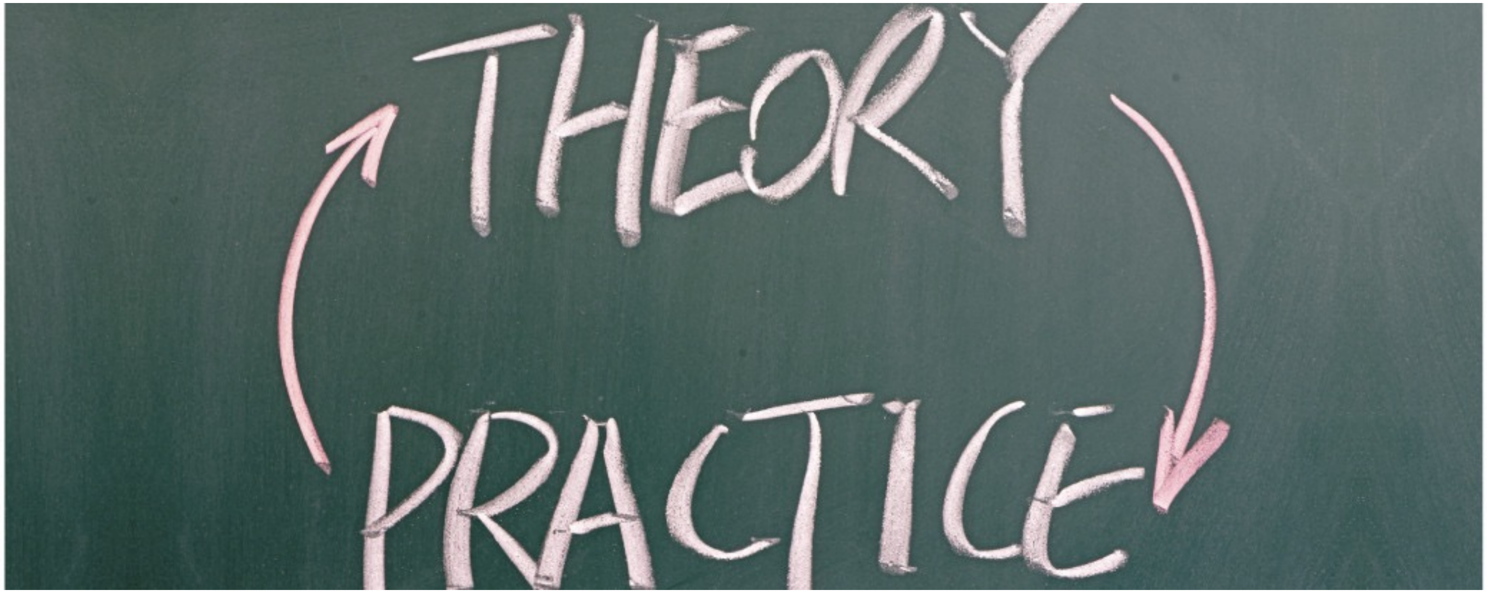
German IT Security Law "1.0"

- 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

Agenda

I. Introduction Information Security
II. Introduction Governance, Risk and Compliance (GRC)
III. Information Security Governance
IV. Information Security Risk Management
V. Information Security Compliance
VI. Hands-on Approach to the Implementation of Information Security GRC

VI. Hands-on Approach to the Implementation of Information Security GRC



mobile business

Chair of Mobile Business & Multilateral Security

Michael Schmid
Goethe University Frankfurt
E-Mail: michael.schmid@m-chair.de
WWW: www.m-chair.de

GOETHE UNIVERSITÄT FRANKFURT AM MAIN