

Implementation of Cybersecurity

How Much We Risk

Cyril Klimeš, Tomáš Pitner

Module Contents

1. Module Summary . . . 2
2. Information Security Management System (ISMS) . . . 3
   2.1. What is ISMS . . . 3
   2.2. PDCA cycle (Plan - Do - Check - Act) . . . 3
   2.3. Plan: Policy, Risks . . . 3
   2.4. Plan: Measures . . . 4
   2.5. Plan: Document . . . 4
   2.6. **Do** . . . 5
   2.7. Do: Processes, Communication . . . 5
   2.8. Check . . . 6
   2.9. Act . . . 6
   2.10. Act: Risk analysis . . . 7
   2.11. Act: Countermeasures . . . 7
   2.12. Documents Required for ISMS Implementation . . . 8
   2.13. Documents Required for ISMS Implementation (2) Risk Assessment . . . 8
   2.14. Documents Required for ISMS Implementation (3) . . . 8
   2.15. ISMS Build-Up . . . 8
   2.16. Maintaining the Security Attributes of Information at the Required Level . . . 9
3. Determination of ISMS objectives . . . 11
   3.1. Examples of SMART goals . . . 11
   3.2. Other activities related to ISMS . . . 11
   3.3. Risk assessment . . . 11
   3.4. Risk assessment of cyber-attack . . . 11
   3.5. Risk assessment of cyber-attack (2) . . . 12
   3.6. Information Security Policy . . . 12
   3.7. Information Security Policy . . . 12
   3.8. Components of IS covered . . . 12
   3.9. Components of IS covered . . . 13
   3.10. Security Policy and Security Documentation . . . 13
   3.11. Security Documentation (2) . . . 13
   3.12. ISMS monitoring . . . 14
   3.13. Change Management . . . 14
   3.14. ISMS control and audit . . . 14
   3.15. Evaluating the effectiveness of the ISMS . . . 14
   3.16. ISMS updates . . . 14
   3.17. "Information Security Policy" document . . . 15
   3.18. "Information Security Policy" document (2) . . . 15
4. Risk Management . . . 16

4.1. Core Questions of Risk Management ISO/IEC 27005:2022 . . . 16
4.2. Questions in PDCA-cycle . . . 16
4.3. Risk Analysis: Terms . . . 17
4.4. Risk Analysis: Types of Threats . . . 18
4.5. Risk management process ISO/IEC 27005:2022 . . . 18
4.6. Risk management in the ISMS process . . . 19
4.7. Risk Analysis . . . 19
4.8. Vulnerabilities . . . 20
4.9. Examples of Vulnerabilities . . . 20
4.10. Threat, Risk . . . 20
4.11. Attack, Impact . . . 20
4.12. Threat . . . 21
4.13. What Characterizes a Threat . . . 21
4.14. Threat Examples . . . 21
4.15. Attack . . . 22
4.16. Types of Attacks (Threats) . . . 22
4.17. Types of Attacks by Strength . . . 22
4.18. Intentional attacks . . . 23
4.19. Attacks Against Data Communication . . . 23
4.20. Relationship Schema for Risk Management in the IS . . . 24
4.21. Acceptable Costs . . . 24
4.22. Procedure of Risk Analysis . . . 25
4.23. Procedure of Risk Analysis (2) . . . 25
4.24. Risk Estimation ISO/IEC 27005:2022 term . . . 25
4.25. Terminology EN-CZ-ISO . . . 26
4.26. Terminology EN-CZ-ISO (2) . . . 26
4.27. Case Study: a Complete Risk Analysis (WEB-SHOP) ISO/IEC 27005:2022 . . . 26

- Expected lecture date WS 2026: **Oct 6**

Chapter 1. Module Summary

- **ISMS**: what it is and why, the PDCA cycle (Plan–Do–Check–Act), SMART objectives, ISMS documentation.
- **Information security policy**: components of information security, policy levels, structure of the policy document.
- **Risk management**: the ISO/IEC 27005:2022 process, its place in the ISMS cycle, the procedure of risk analysis.
- **Vulnerabilities and threats**: types of threats, vulnerability examples, threat vs. risk vs. attack vs. impact.
- **Attacks**: intentional attacks, types and strength of attacks, attacks against data communication.
- **Risk estimation**: likelihood and impact, ISO/IEC 27005:2022 terminology (EN–CZ–ISO), acceptable costs of protection.
- **Case study (WEB-SHOP)**: a complete worked risk analysis — asset valuation, `R = T x A x V`, risk levels, and controls.
- **Core questions of risk management** and where they belong in the individual PDCA phases.

Chapter 2. Information Security Management System (ISMS)

2.1. What is ISMS

- Information Security Management System (**ISMS**) ISO 27001:2022 is a framework of policies, procedures, guidelines, associated resources and activities to achieve the stated objectives of an organization.



- It is based on the **PDCA** cycle (*Plan-Do-Check-Act*) and on the risk management approach of the information and communication system.
- It specifies how to establish, implement and operate, monitor and review, maintain and improve information and data security, following the international standard ISO/IEC 27001:2022 ISO 27001:2022.

2.2. PDCA cycle (Plan - Do - Check - Act)

- PDCA Model for *Information Security Management* ISO 27001:2022

2.3. Plan: Policy, Risks

Establish the framework, scope, risk approach, and controls

- Information Security Management Systems (ISMS) **scope** definition
- Identify relevant **legal**, regulatory, and contractual requirements
- ISMS **policy** definition
- Definition of the **risk assessment approach**
- Identification of **risks**
- Risk **assessment**
- Identification and assessment of conditions for **risk treatment**

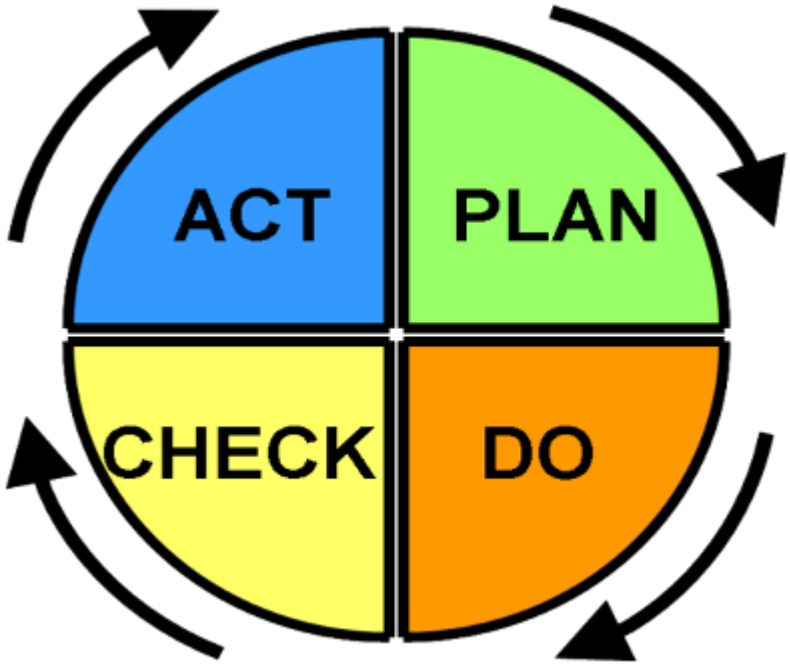


Figure 1. Plan

2.4. Plan: Measures

Security measures

- Selection of security **measures** and their objectives
- Preparation of the SOA (**Statement of Applicability**) document
- Obtain management **approval** and **commitment**
- Identification of all selected measures
- Justification for the choice (positive and negative) in the light of the risk assessment
- Follows up on the results of the risk assessment and countermeasure implementation plan

2.5. Plan: Document

Document countermeasures

- Document the selected **countermeasures** (existing and planned) to cover the risks (mitigation, elimination, acceptance) and the **rationale** for the selection (according to ISO/IEC 27002:2022) ISO 27002:2022

Dates for implementation

- Determines the **dates** for the implementation of the planned measures
- Separate document only in case of subsequent **certification** or for large IS of large organizations

2.6. Do

Policies & Risk treatment

- Implement and operate security **policies and controls**
- Carry out the **risk treatment plan** (technical, organizational, administrative measures)
- Establish organizational **structure**, **roles**, and **responsibilities**
- Conduct **training and awareness** programs for staff

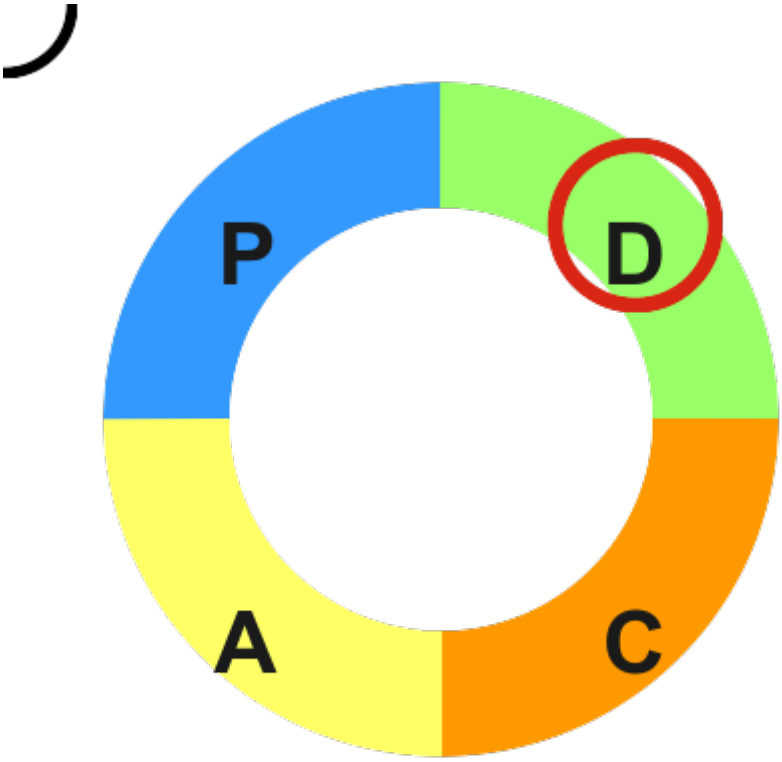


Figure 2. Do

2.7. Do: Processes, Communication

Operational processes and procedures

- access control management
- change management
- incident management
- backup and recovery

Communication

- Ensure internal and external communication

Asset operation

Operate and manage information assets according to their classification

2.8. Check

Monitoring

- Implementation of monitoring
- Regular reviews of the effectiveness of the ISMS
- Review of the level of acceptable and residual risks
- Performing internal ISMS audits
- Managing reviews of effectiveness and risk levels
- Keeping records of events and incidents with an impact on the ISMS

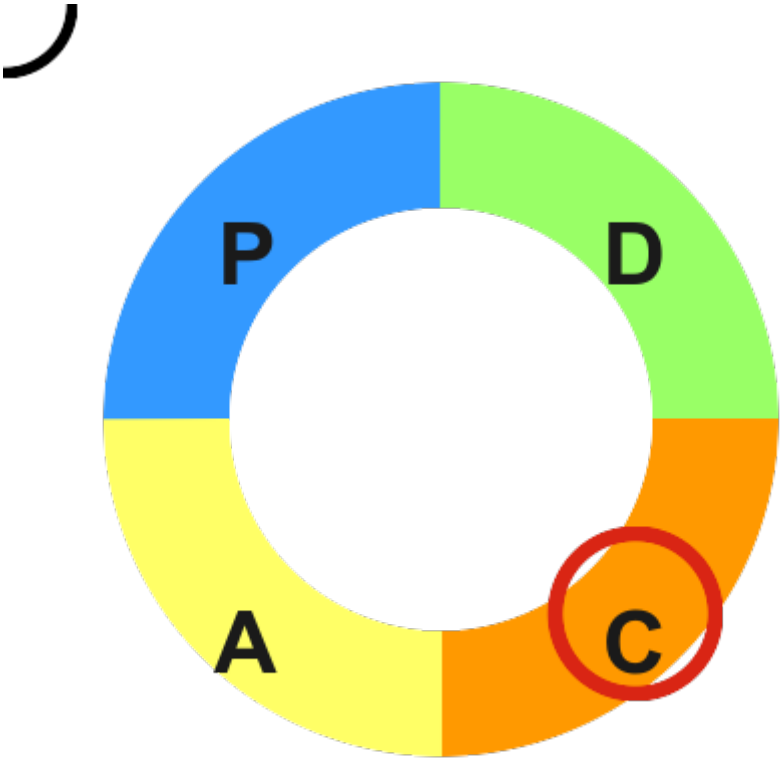


Figure 3. Check

2.9. Act

- Implement if the changes have led to success
- Improving ISMS
- Corrective action
- Determining the scope of the ISMS in the organisation
- ISMS Basic Policy

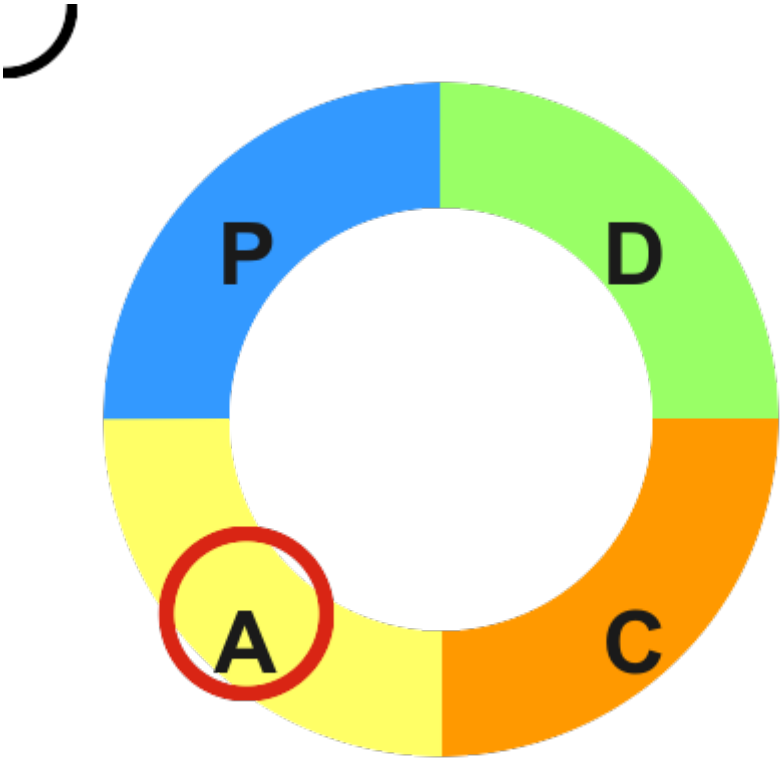


Figure 4. Act

2.10. Act: Risk analysis

Update risk analysis:

- Risk assessment
- Definition and description of the risk assessment approach
- Identification and valuation of assets
- Identification of risks
- Risk analysis

2.11. Act: Countermeasures

Update countermeasures:

- Proposal for countermeasures
- Objectives of measures and safety measures to manage risks
- Acceptance of risks
- Declaration of support by the management of the organisation for the implementation and operation of the ISMS
- Declaration of applicability

2.12. Documents Required for ISMS Implementation

1. Determination of the scope of the ISMS within the organization
2. Basic ISMS policy
3. Risk assessment

2.13. Documents Required for ISMS Implementation (2) Risk Assessment

a. Definition and description of the risk assessment approach
b. Identification and evaluation of assets
c. Identification of risks
d. Risk analysis
e. Design of countermeasures
f. Objectives and security controls for risk treatment
g. Risk acceptance

2.14. Documents Required for ISMS Implementation (3)

4. Management statement of support for the implementation and operation of the ISMS
5. Statement of Applicability (SoA)

Management statement — a declaration by top management that it approves the ISMS and commits to its implementation and operation.

Statement of Applicability (SoA) — the list of the security controls selected on the basis of the risk assessment, together with the justification for their selection and for excluding any controls of Annex A of ISO/IEC 27001:2022; it is a **mandatory output** of the ISMS.

2.15. ISMS Build-Up

- **Procedure for the design and implementation of the ISMS** — determining the scope of the ISMS, the ISMS policy, the risk assessment, the Statement of Applicability, and the implementation of the selected measures.
- **Feedback enabling continual improvement of the ISMS** — the results of monitoring, internal audits, and the evaluation of effectiveness are fed back into the next *Plan* phase.

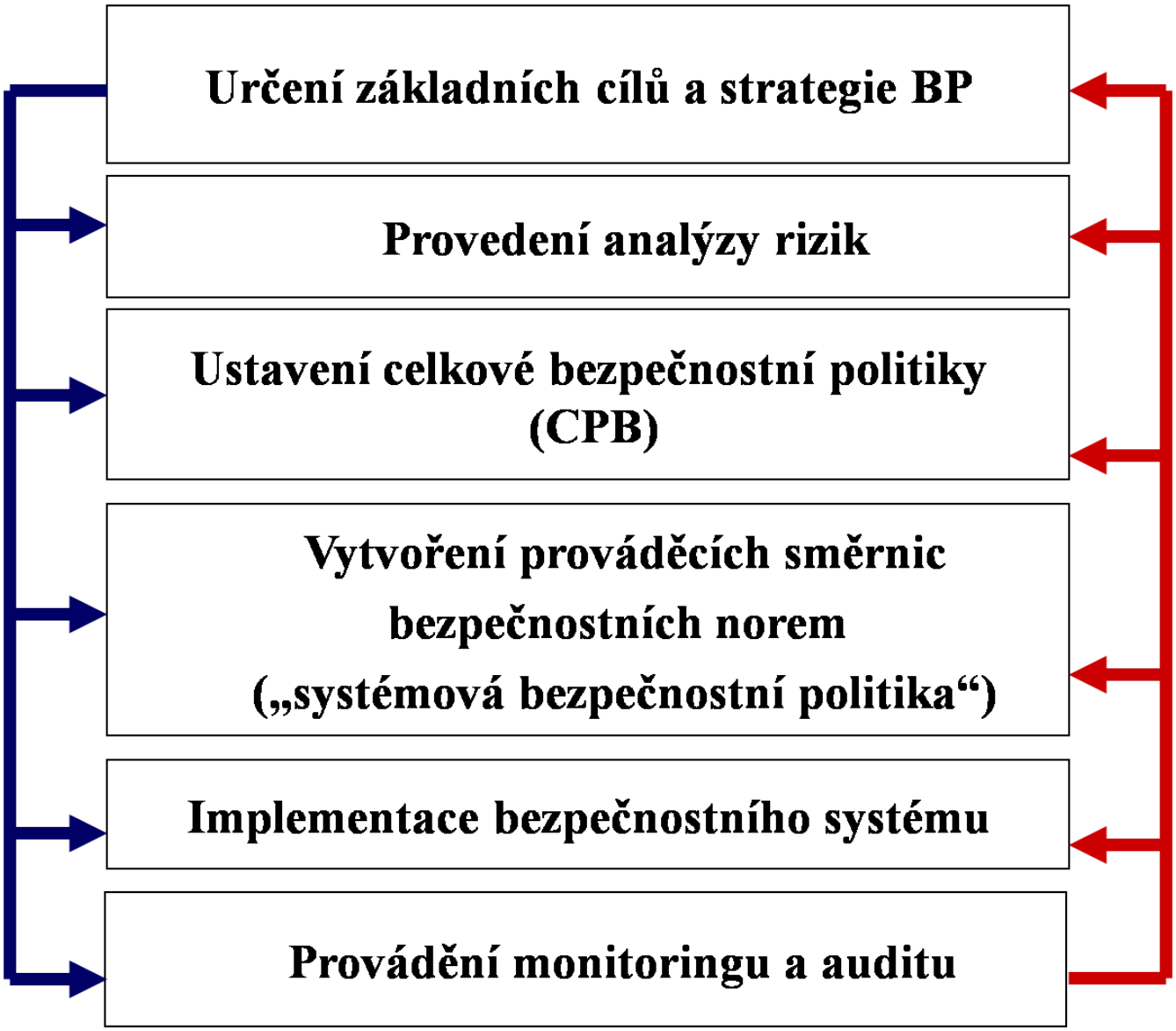


Figure 5. ISMS Build-Up

The build-up of the ISMS is the *Plan—Do—Check—Act* cycle applied to the whole management system: each pass through the loop widens the scope and improves the set of measures.

2.16. Maintaining the Security Attributes of Information at the Required Level

Fundamental objective of the ISMS — keeping the security attributes of information at a **defined level**.

Security attribute	What is maintained
Confidentiality	information is not disclosed to unauthorized subjects (the **CIA triad** is defined in module 01)
Integrity	information is accurate, complete, and protected against unauthorized modification
Availability	information and related services are accessible to authorized subjects when required

Security attribute	What is maintained
Authenticity	the origin of the information is genuine and verifiable
Reliability	the information and the processing that produced it are trustworthy and consistent
Provability of origin	it can be proven who created and sent the information (non-repudiation of origin)
Provability of receipt	it can be proven that the information was delivered and received (non-repudiation of receipt)

Information must be protected in the context of the fundamental security objectives at a **defined level**.

Chapter 3. Determination of ISMS objectives

ISMS objectives must be SMART

S - Specific	as precise as possible to make it clear what is meant by the objective.
M - Measurable	to assess the extent to which the objective has been met.
A - Accepted	accepted by the responsible person.
R - Realistic	realistic so that it can be achieved in real time.
T - Timed	timed to make it clear when the goal is to be met.

3.1. Examples of SMART goals

- Percentage reduction in the number of workstation infections caused by the user (antivirus solutions on workstations, mail servers and user education).
- Preventing information leakage (proper deployment of DLP (Data Loss Prevention).
- Speeding up system recovery time after a failure (business continuity solutions).
- Streamlining and accelerating the resolution of security incidents (deploying a security incident management environment).

3.2. Other activities related to ISMS

- Risk assessment,
- Security policy making,
- ISMS monitoring,
- Change management,
- Control and audit
- Evaluating the effectiveness of the ISMS

3.3. Risk assessment

- Procedure for identifying potential security risks and determining their values
- Example: cyber attack on a server Information Security Policy

3.4. Risk assessment of cyber-attack

Table 1. Risk assessment of cyber-attack

Category	Description
Risk identification	Cyber-attack on Webserver
Probability	4 (high)

Category	Description
Impact	5 (very high)
Total risk score	20 =4*5
Countermeasures	setup advanced firewalls, regular updates

3.5. Risk assessment of cyber-attack (2)

Table 2. Risk treatment

Category	Description
Risks	Identification of risks
Responsible person	IT security team
Countermeasures	Design of countermeasures
State	in progress

3.6. Information Security Policy

defines:

- Purpose and scope
- Roles and responsibilities
- Security measures
- Incident Management
- Monitoring and review

3.7. Information Security Policy

- IT Security Policy (ISP) is the fundamental document of information security.
- ISP is a set of technical and administrative measures and procedures, serving to maintain the defined level of security.
- It is developed based on a **risk analysis** (RA).

3.8. Components of IS covered

Components of the IS covered by the ISP = **assets**:

IT

- Hardware (computers, servers, printers),
- Software (operating systems, applications),
- Telecommunication and network equipment (routers, switches, cabling, …)

People

- employees including system and network administrators,
- customers or clients,
- business partners, etc.

3.9. Components of IS covered

Processes

- workflows,
- activities,
- services, …

Data

- **enterprise information** in different stages of processing:
- input reports, databases, transmitted data packets, output reports, …

3.10. Security Policy and Security Documentation

Decree No. 409/2025 Coll., Sections 3(d) and 6 (management of the security policy and security documentation)

Security Policy

- A set of principles and rules that determine how assets are protected (Section 2(d))
- States the **main principles**, the objectives of the ISMS, the **security needs** and the **rights and obligations** related to information security management
- Long-term, independent of current ICT, in line with the strategic direction of the organization

Security Documentation

- Detailed documentation for the individual security measures (Sections 3 to 27) — e.g. asset, risk, supplier, human resources, change and access management, incident handling, continuity, physical and network security, cryptography
- Derived from the security policy, the security needs and the results of the risk assessment
- Dynamic — reviewed regularly, kept up to date and reflected in operational documentation, rules and procedures



The security policy and documentation must be managed so that they are

- available in electronic or paper form,
- brought to the attention of the persons concerned,
- adequately accessible to them,
- protected in terms of confidentiality, integrity and availability, and
- complete, legible, easily identifiable and searchable.

The security policy and documentation cover, among other things

- **monitoring and auditing**: continuous and subsequent monitoring of the effectiveness of the information security system,
- the **recovery plan** and
- the **emergency plan**.

3.12. ISMS monitoring

- Regular auditing
- Incident tracking
- Control of recovery plans
- Tracking changes
- Employee education and awareness
- Risk analysis

3.13. Change Management

What is Significant change:

- may have an impact on cyber security
- poses a high risk regardless of the measures already in place
- E.g. change of configuration, functionality, major supplier
- Significant changes need to be managed.

3.14. ISMS control and audit

- a tool to ensure effective improvement of the established ISMS
- highlighting any deviations from *best practice*

3.15. Evaluating the effectiveness of the ISMS

- Assessment of the status of the ISMS, including a review of the risk assessment,
- assessing the results of audits performed and the impact of cyber security incidents on the defined scope of the ISMS.

3.16. ISMS updates

- Based on the results of the evaluation of the effectiveness of the ISMS, the findings of audits and in connection with significant changes, the ISMS and the relevant documentation must be updated.

3.17. "Information Security Policy" document

- Information security objectives and principles
- Legislative framework
- Scope of the information management system

Implementation of ISMS:

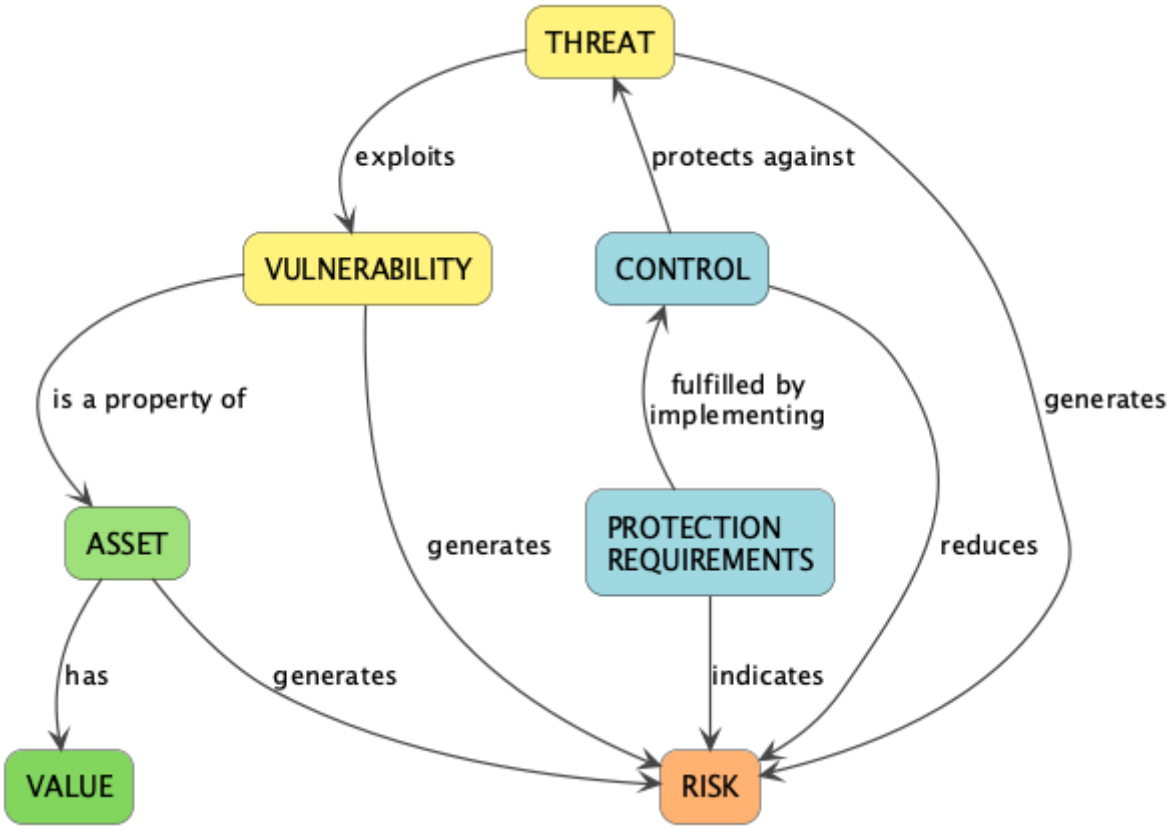
- CS committee,
- CS manager,
- CS architect,
- CS auditor,
- asset guarantor,
- RACI matrix

3.18. "Information Security Policy" document (2)

Information security management processes and principles

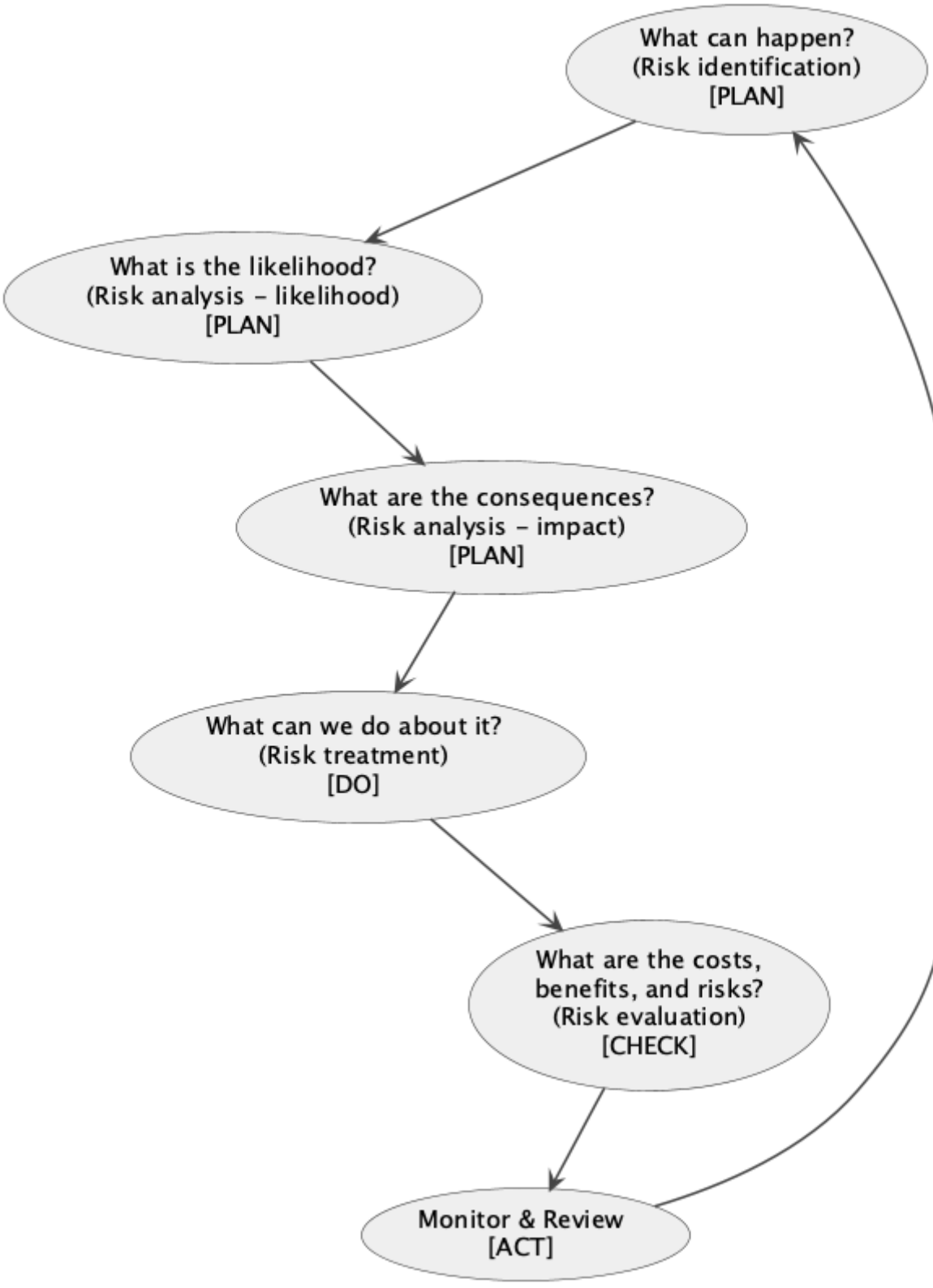
asset classification and management, asset evaluation criteria, human resource management, physical security management, preventive and corrective action management, communications and operations security management, access management, systems development and maintenance, business continuity management, information security compliance, information security responsibilities, reviews and audits

Chapter 4. Risk Management



4.1. Core Questions of Risk Management ISO/IEC 27005:2022

1. What can happen? **(Risk identification – identifying potential events or threats)**
2. What is the likelihood that it will happen? **(Risk analysis – estimating probability/likelihood)**
3. What are the consequences if it happens? **(Risk analysis – estimating impact/consequences)**
4. What can we do about it? **(Risk treatment – selecting and implementing measures)**
5. What are the costs, benefits, and risks of each option? **(Risk evaluation – comparing options and making decisions)**



4.3. Risk Analysis: Terms

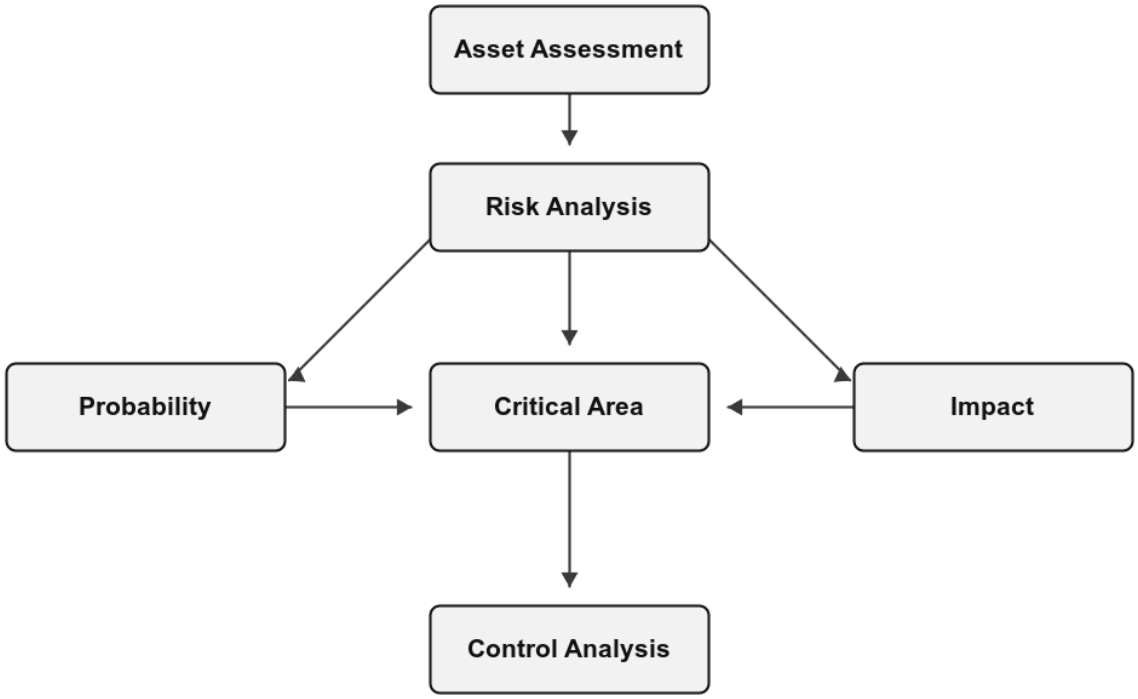
Asset	anything that has value for the company and should be protected accordingly
Threat	any event that could cause a breach of the confidentiality, integrity, and availability of an asset
Vulnerability	a property of an asset or a weakness in physical, logical, or administrative

	security that could be exploited by a threat.
Risk	the probability that a threat will exploit a vulnerability and cause a breach of confidentiality, integrity, or availability.
Countermeasure	a measure at the physical, logical, or administrative security level that reduces vulnerability and protects an asset from a given threat

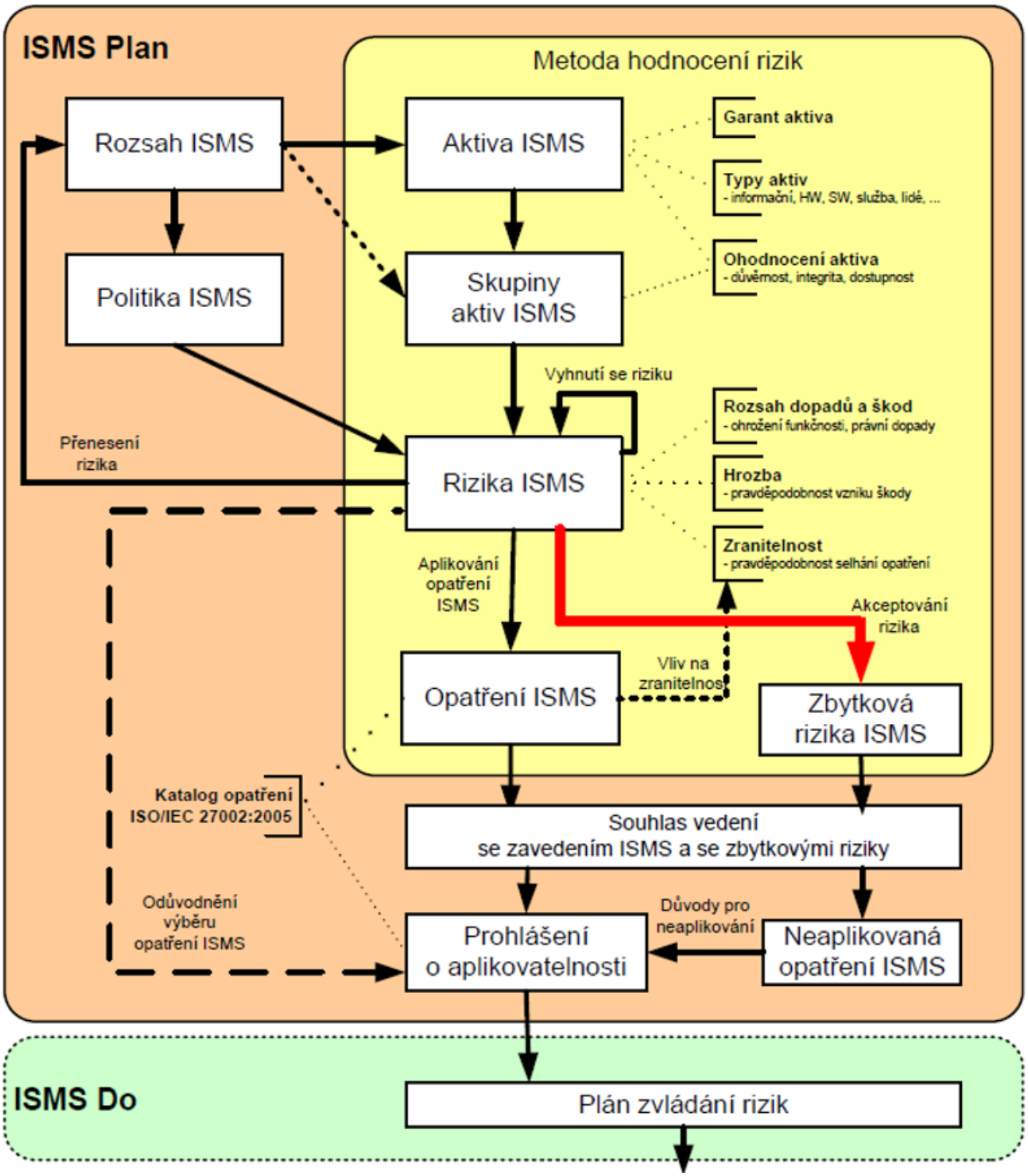
4.4. Risk Analysis: Types of Threats

Physical	• Natural influences • HW failure • Power outage
Software	• External • SW errors
People	• Intentional
Internal	• Unintentional • External

4.5. Risk management process ISO/IEC 27005:2022



4.6. Risk management in the ISMS process



4.7. Risk Analysis

- **Risk Analysis** is a key step in building an ISMS.

Key Questions of Risk Analysis

- What will happen if the information is not protected? (**impact on IS**)
- How can information security be compromised? (**possibility of exploiting a vulnerability** by a threat — carrying out an attack)

- What is the probability of this happening? (**degree of risk**)

4.8. Vulnerabilities

- **Vulnerability** is a property of an IS (imperfection of the IS or its components).
- Principle: there is no IS without vulnerabilities.

Occurrence of vulnerabilities:

- **HW**
- **SW**
- Operating **environment**
- **People** (employees and other authorized users)

The goal of RA

- to **identify** vulnerabilities
- to **determine** the acceptable level of risk resulting from the existence of vulnerabilities
- to determine how to **keep risks** at an **acceptable** level

4.9. Examples of Vulnerabilities

- Inadequate **maintenance** of the information and communication system,
- **obsolescence** of the information and communication system,
- inadequate **protection** of the external perimeter,
- inadequate **security awareness** of users and administrators,
- Inappropriate **access rights** settings,
- Inadequate procedures for **identifying and detecting** negative security phenomena, cyber security events and cyber security incidents.

4.10. Threat, Risk

Threat

(primary, non-derived phenomenon) creates the possibility of exploiting a vulnerability

Risk

is the probability of exploiting a vulnerability (probability of a threat occurring)

4.11. Attack, Impact

Attack

- (security incident) is the exploitation of a vulnerability.
- *Intentional* attack (subjective attack)

- *Unintentional* attack (objective attack)

Attack targeted to specific security attribute

Interruption	against availability
Eavesdropping	against confidentiality
Change	against integrity
Forgery (falsification)	against authenticity

4.12. Threat

Consequence of IS vulnerability

- Possibility of exploiting vulnerability
- Creates a risk of attack

Objective threat

- arises from the environment
- natural, physical
- physical
- technical, logical

Subjective threat

- arises from human action
- intentional
- unintentional

4.13. What Characterizes a Threat

Frequency

criticality of application (for both objective and subjective threats)

Motivation

abilities, financial resources, time resources of the potential attacker (for subjective threats)

Type of potential attacker

employee with malicious intent, employee unintentionally performing malicious activities, *external attacker*: former employee, hacker, layman, "script kiddy", hired professional, competitor, psychopath, etc.

4.14. Threat Examples

- **Violation** of the security policy, **execution** of unauthorized activities, **misuse** of **privileges** by users or administrators

- **Damage** to or **failure** of technical or software equipment
- **Identity misuse**
- Use of software **contrary to license** conditions
- **Malicious** code (e.g. viruses, spyware, trojans)
- Breach of **physical security**
- **Interruption** of electronic communication services or electricity supply
- Misuse or **unauthorized modification** of data

4.15. Attack

- An attack is the realization of a threat.

Synonyms of attack

- Security incident
- IS failure (objective causes)
- IS compromise (result of a subjective threat)

ISO/IEC 27005:2022 — definitions of threat, event, incident.

ISO/IEC 27032:2012 (Cybersecurity — Guidelines) — defines cyberattack explicitly as "an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset."

ISO/IEC 27005:2022 (Information security risk management) — threat sources, threat events, and their relationship to risks and incidents.

4.16. Types of Attacks (Threats)

Categories according to:

- **Strength** and impact level (*weak, medium, strong*)
- **Target** (*data, hardware, software*)
- **Source** (*internal, external*)
- **Activity** (*active* — data are modified, *passive* — data are not modified)
- **Intention** (*intentional* — deliberate, *unintentional* — accidental)
- **Motivation**
- **Type of impact** (loss of *confidentiality*, *availability*, *integrity*, *authenticity*)

4.17. Types of Attacks by Strength

Catastrophic

leading to the collapse of the organization or to its criminal liability

Significant
: causing serious damage to the organization

Insignificant
: causing minor or negligible damage

4.18. Intentional attacks

- The strength of the attack is related to the level of time, money, knowledge, etc. invested:

  Weak attacker
  : amateur, accidental, script kiddie, etc.

  Medium-strength attacker
  : hackers with knowledge and time, usually without significant financial resources

  Strong attacker
  : professionals (industrial espionage, intelligence services, etc.)

4.19. Attacks Against Data Communication

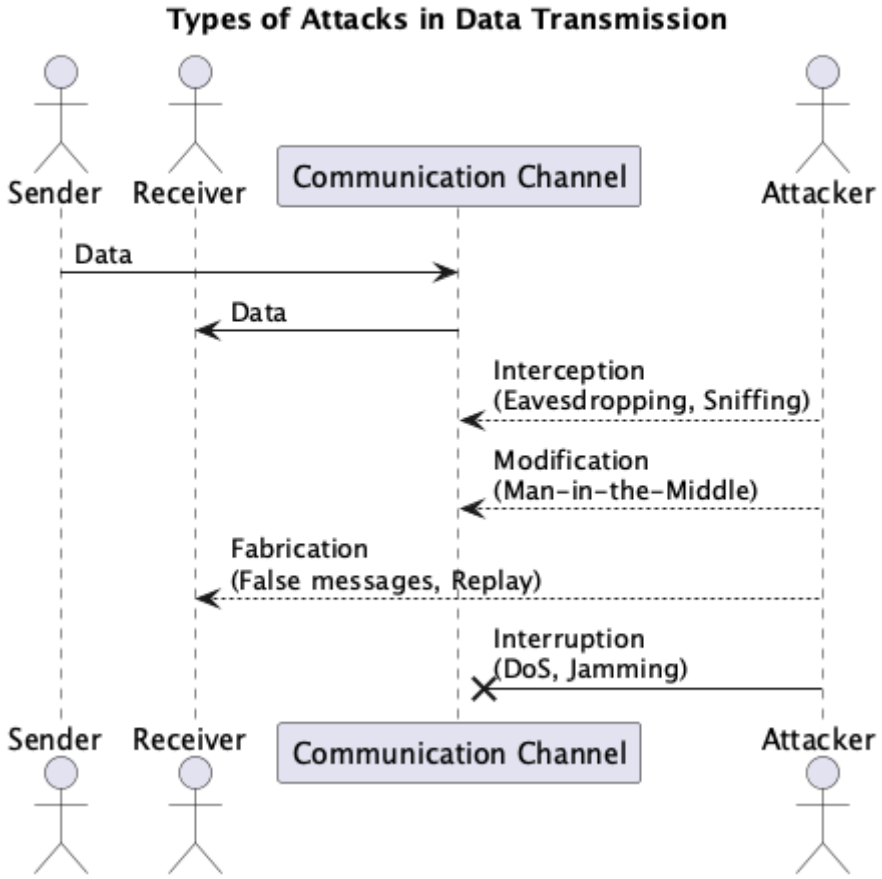
ISO/IEC 27033 Network Security defines:

Interception attacks
: eavesdropping, sniffing, wiretapping

Modification attacks
: altering data in transit, man-in-the-middle (MITM)

Fabrication attacks
: injecting false messages, spoofing, replay attacks

Interruption attacks
: denial of service (DoS), jamming, cutting communication links



4.20. Relationship Schema for Risk Management in the IS



Figure 6. Relationship Schema for Risk Management in the IS

4.21. Acceptable Costs

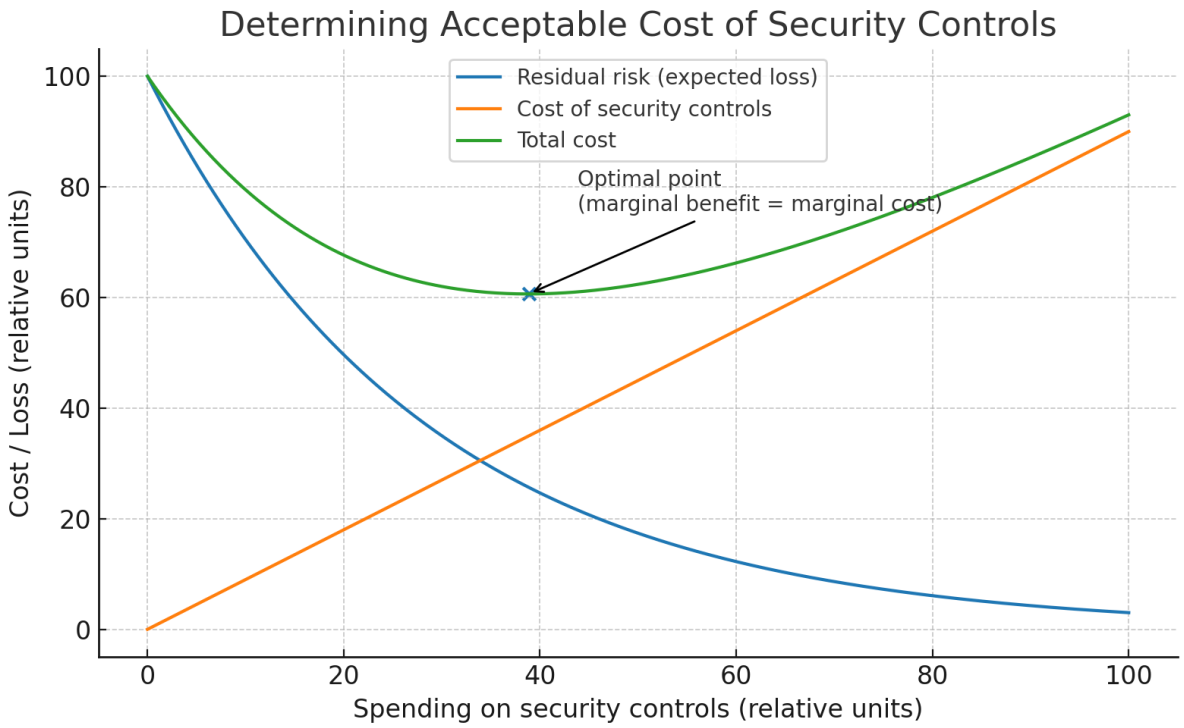


Figure 7. Acceptable Cost of Security Controls

4.22. Procedure of Risk Analysis

1. Determination of the scope of the risk analysis (RA) **Reference:** ISO/IEC 27005:2022, 6 — Context establishment
2. Identification and valuation of assets **Reference:** ISO/IEC 27005:2022, 7.2 — Risk identification (assets)
3. Identification of vulnerabilities — critical areas **Reference:** ISO/IEC 27005:2022, 7.2 — Risk identification (vulnerabilities)
4. Risk estimation **Reference:** ISO/IEC 27005:2022, 7.3 — Risk analysis
5. Determination of unacceptable and acceptable risks **Reference:** ISO/IEC 27005:2022, 7.4 — Risk evaluation
6. Determination of expected annual losses **Reference:** ISO/IEC 27005:2022, Annex A — Risk assessment techniques (e.g. ALE)
7. Identification of applicable security measures (SM) to reduce risks to an acceptable level **Reference:** ISO/IEC 27005:2022, 8.2 — Risk treatment options
8. Estimation of annual savings after implementing security measures into the IS **Reference:** ISO/IEC 27005:2022, 8.6 — Risk treatment plan, cost-benefit analysis

4.24. Risk Estimation ISO/IEC 27005:2022 term

Asset

Description of the asset being assessed.

Impact value (1-5)

Assessment of the impact that exploitation of this asset would have.

Threat value (1-5)

Likelihood that a threat will affect this asset.

Vulnerability value (1-5)

Likelihood that a vulnerability will be exploited.

Overall risk score

Calculation of the risk score as the product of the impact value, the threat value, and the vulnerability value. `Risk = impact x threat x vulnerability`

Control (Treatment measure)

Proposed measures to reduce the risk.

4.25. Terminology EN-CZ-ISO

Term (CZ)	Term (EN)	ISO/IEC Reference
Aktivum	Asset	ISO/IEC 27002:2022, 3.1.2 - asset
Dopadová hodnota (1-5)	Impact value (1-5)	ISO/IEC 27005:2022, 3.1.14 - consequence
Hodnota hrozby (1-5)	Threat value (1-5)	ISO/IEC 27005:2022, 3.1.13 - likelihood of threat occurrence
Hodnota zranitelnosti (1-5)	Vulnerability value (1-5)	ISO/IEC 27005:2022, 3.1.13 - likelihood of vulnerability exploitation

4.26. Terminology EN-CZ-ISO (2)

Term (CZ)	Term (EN)	ISO/IEC Reference
Celkové rizikové skóre	Overall risk score	ISO/IEC 27005:2022, 7.3.4 — determining the levels of risk (semi-quantitative scoring method)
Riziko = dopad × hrozba × zranitelnost	Risk = impact × threat × vulnerability	ISO/IEC 27005:2022, Annex A — examples of risk assessment techniques
Opatření	Control / Risk treatment measure	ISO/IEC 27005:2022, 8.2 — risk treatment options; ISO/IEC 27005:2022, 3.1.16 — control

4.27. Case Study: a Complete Risk Analysis (WEB-SHOP) ISO/IEC 27005:2022

The fictional company **WEB-SHOP** sells goods online. It has its own office, from which the company is managed, and a warehouse for the goods sold, which is located at a different site than the office. The example below goes through the whole calculation: asset valuation, threat and vulnerability

assessment, the risk value, the risk level, and the proposed controls.

Identified Assets and Their Valuation

The most important assets are marked **5**.

Asset	Value (A)	Note
Information (customers, orders, goods)	5	the core business data
Server database	5	order and customer data
Hardware — servers	5	the technical foundation of the e-shop
Data in transit between the office and the warehouse	5	traffic over the public network
Warehouse database	4	stock and logistics data
Software — operating systems	4	
Software — database systems	4	
Services — server connection	4	availability of the e-shop
Office and warehouse network	3	connectivity between the two sites

Identified Threats and Associated Vulnerabilities

Threat	Vulnerability	Likelihood (T)	Vulnerability (V)
Malware / ransomware	missing or obsolete antimalware, unpatched system	4	4
Phishing / social engineering	insufficient security training of employees	3	5
Unauthorized modification of data	weak access control, no logging	3	4
Network intrusion / interception	unprotected public network connection	3	5
Hardware failure	no redundancy of the critical servers	2	3
Power outage	no UPS / backup power source	3	4
Theft of a server	warehouse on a separate site with weak physical security	1	3

Risk Analysis Table

The risk value is the product **R** = **T** × **A** × **V**, where **T** is the likelihood of the threat, **A** the value of the asset, and **V** its vulnerability (each on a 1—5 scale).

Asset — threat	A	T	V	R = A × T × V	Level
Information — unauthorized modification	5	3	4	60	MRV
Server database — malware / ransomware	5	4	4	80	HRV
Data in transit — interception	5	3	5	75	HRV
Hardware — servers — theft	5	1	3	15	LRV
Operating systems — network intrusion	4	3	4	48	MRV
Database systems — unauthorized modification	4	3	3	36	MRV
Services — server connection — denial of service	4	3	3	36	MRV
Warehouse database — power outage	4	3	4	48	MRV
Employees — phishing	4	3	5	60	MRV

For example, for the **server database** threatened by **malware**: **R = A × T × V = 5 × 4 × 4 = 80**, i.e. a **high risk value (HRV)**. For **theft of a server**: **R = 5 × 1 × 3 = 15**, i.e. a **low risk value (LRV)**.

Scales Used in the Example

Likelihood of the risk (T)

- **Low likelihood (LL)** — a likelihood below 33 %,
- **Medium likelihood (ML)** — a likelihood of 33—66 %,
- **High likelihood (HL)** — a likelihood above 66 %.

Impact if the risk occurs

- **Minor adverse impact (MAI)** — damages of up to 0.5 % of the total project value,
- **Medium adverse impact (MeAI)** — damages of 0.51—19.5 % of the project value,
- **Major adverse impact (MjAI)** — damages above 20 % of the project value, a threat to the project objective and deadline.

Risk value ® in this example

- **Low risk value (LRV)** — R ≤ 20; the risk may occur at any time and will be mitigated or eliminated by the proposed control,
- **Medium risk value (MRV)** — R = 21—60; the risk endangers the delay of a part of the project and is mitigated rather than eliminated, with an impact on resources and costs,
- **High risk value (HRV)** — R > 60; the risk endangers the whole project; the controls can mitigate but not eliminate it.

Proposed Controls (Implementation of Mechanisms)

Risk (asset — threat)	Proposed control
Information — unauthorized modification	role-based access control (RBAC), audit logging, encryption
Server database — malware / ransomware	antivirus / EDR, patching, network segmentation, regular verified backups
Data in transit — interception	TLS/VPN for the connection between the sites, PKI
Hardware — servers — theft	mechanical barriers, electrical intrusion alarm, camera system
Operating systems — network intrusion	firewall, IDS/IPS, hardening, secure network topology
Database systems — unauthorized modification	RBAC, database audit
Services — server connection — denial of service	redundancy, load balancing, DDoS protection
Warehouse database — power outage	UPS, backup power source, regular verified backups
Employees — phishing	security awareness training, e-mail filtering, multi-factor authentication

The Fraud Detection System (FDS) and DLP (Data Loss Prevention) complement the controls above for the detection of fraudulent transactions and the prevention of data leakage.