

Implementation of Cybersecurity

What We Protect and by What Rule

Cyril Klimeš, Tomáš Pitner

Module Contents

1. Module Summary . . . 2
2. The goal of cybersecurity . . . 3
   2.1. Preventive measures . . . 3
   2.2. Aspects for implementing cybersecurity . . . 3
   2.3. Aspects for implementing cybersecurity (cont.) . . . 4
   2.4. Information protection CIA triad . . . 4
   2.5. CIA Examples . . . 4
   2.6. ISMS objectives . . . 4
   2.7. Cybersecurity legislation in CZ . . . 5
   2.8. New implementing decrees . . . 5
   2.9. Key changes under the NIS2 framework . . . 6
   2.10. Original framework (repealed on 1 Nov 2025) . . . 6
   2.11. Cybersecurity legislation in EU . . . 6
   2.12. ISMS - Information Security Management System . . . 6
   2.13. ISMS Diagram (ISO 27000) . . . 7
   2.14. Information security management model [ISO27001] . . . 7
   2.15. Information security areas [ISO27002] . . . 8
   2.16. Why implement CS? . . . 8
   2.17. What is cybersecurity implementation? . . . 9
   2.18. What is cybersecurity implementation? (2) . . . 9
3. Security measures - organizational areas . . . 10
   3.1. Management and ISMS . . . 10
   3.2. Assets, risks, and suppliers . . . 10
   3.3. Operations and change . . . 10
4. Security measures - technical areas . . . 11
   4.1. Infrastructure and access . . . 11
   4.2. Detection and response . . . 11
   4.3. Cryptography, availability, and special systems . . . 11
   4.4. Measure Areas and Course Modules . . . 11
   4.5. Measure Areas and Course Modules (2) . . . 12
5. Cybersecurity Policies . . . 13
   5.1. Cybersecurity Policies (2) . . . 13
   5.2. Cybersecurity Policies (3) . . . 13
   5.3. The Systemic Security Policy (SSP) . . . 13
   5.4. Structure of the Organization’s Security Documentation . . . 14
   5.5. Example of a security document . . . 14
   5.6. Security documentation . . . 15
   5.7. Emergency plan . . . 15

5.8. Summary: Security implementation . . . 15
6. Asset Management . . . 16
6.1. Asset Properties . . . 16
6.2. Division of Assets . . . 16
6.3. Asset Identification and Inventory ISO 27002:2022 . . . 17
6.4. Asset Roles . . . 17
6.5. Asset Ratings . . . 17
6.6. Availability Rating (Low, Medium) . . . 17
6.7. Availability Rating (High, Critical) . . . 18
6.8. Confidentiality Assessment: Low . . . 18
6.9. Confidentiality Assessment: Medium . . . 18
6.10. Confidentiality Assessment: High . . . 18
6.11. Confidentiality Assessment: Critical . . . 19
6.12. Asset Catalog . . . 19
6.13. Assessment of the Importance of Primary Assets . . . 19
6.14. Classification of Assets . . . 20
6.15. Asset Disposal Rules . . . 20
6.16. Asset Disposal Rules (2) . . . 20
6.17. Disposal Levels . . . 21
6.18. Disposal: Example . . . 21
6.19. Information on Human-readable Media . . . 21
6.20. Mobile Devices . . . 22
6.21. Network Devices . . . 22
6.22. Magnetic Media . . . 23
6.23. Electronic Media . . . 23
6.24. Outsourcing and Cloud . . . 23

- Expected lecture date WS 2026: **Sep 22**

Chapter 1. Module Summary

- **Goal of cybersecurity**: effective measures against unauthorized access and attacks; information security in *all* forms (digital, physical, verbal); people, processes, technologies.
- **Czech legal framework**: Act No. 264/2025 Coll. (in force since 1 Nov 2025, transposes NIS2) with the implementing decrees Nos. 334/2025 and 408–412/2025.
- **EU framework**: NIS2, DORA, CER, Cybersecurity Act, Cyber Resilience Act.
- **Measure areas**: organizational and technical security measures, mapped onto the six course modules.
- **Security policy**: policy layers, security documentation, emergency plan, steps of implementation.
- **ISMS**: ISO/IEC 27001:2022 in the PDCA model, ISO/IEC 27002:2022 areas, objectives, documentation.
- **Asset management**: division and identification of assets, inventory, classification and rating, asset catalog, disposal rules and levels.

Chapter 2. The goal of cybersecurity

- Implementation of effective measures to protect computers and computer networks from unauthorized access or attack.
- **Cybersecurity** focuses on protecting systems, networks, and data from digital attacks originating in cyberspace.
- **Information security** is broader; it aims to protect information in *all forms* (digital, physical, verbal)
- It is necessary to interconnect *people*, *processes*, and *technologies*.

2.1. Preventive measures

- **employee training**,
- **software protection** of **networks**, **clouds**, **applications**, **data**, and **information**,
- **database and infrastructure security**,
- **mobile device security** (**phones**, **tablets**),
- **physical security** of **information**,
- **operational security**,
- data **backup**,
- data **recovery** after an **attack**.

2.2. Aspects for implementing cybersecurity

Technological measures

Installation and maintenance of security software, such as antivirus programs, firewalls, and intrusion detection systems.

Organizational measures

Creation of security policies and procedures that define how employees should behave and what steps they should take in the event of a security incident.

Monitoring and auditing

Regular monitoring of systems and conducting audits to help identify weaknesses and ensure that security measures are effective.

Data backup and recovery

Regularly backing up important data and planning for disaster recovery so that operations can be quickly restored in the event of an attack or system failure.

2.3. Aspects for implementing cybersecurity (cont.)

Training and education

Regular training of employees on current threats and best practices so that they are able to recognize and respond to potential attacks.

Legal and regulatory compliance

Complying with relevant laws and regulations related to data protection and cybersecurity.

2.4. Information protection CIA triad

Confidentiality	The property that characterizes that information is not accessible or disclosed to unauthorized individuals, entities, or processes.
Availability	The property of accessibility and usability upon request by an authorized person.
Integrity	The property of protecting the accuracy and completeness of data. The assurance that data has not been altered.

- Understanding the CIA Triad
- Data Integrity

2.5. CIA Examples

Confidentiality	• Meaning: Only the right people can access the information held by the organization. • Risk example: Criminals get hold of your clients' login details and sell them on the Darknet.
Information integrity	• Meaning: Data that the organization uses to pursue its business or keeps safe for others is reliably stored and not erased or damaged. • Risk example: A staff member accidentally deletes a row in a file during processing.
Availability of data	• Meaning: The organization and its clients can access the information whenever it is necessary so that business purposes and customer expectations are satisfied. • Risk example: Your enterprise database goes offline because of server problems and insufficient backup.

- ISO 27001 CIA Examples

2.6. ISMS objectives

Identification and protection of information assets

Determining which assets need to be protected and implementing measures to protect them.

Risk management

Identifying, assessing, and managing risks associated with information assets.

Control and monitoring

Regular monitoring and control of the measures put in place to ensure their effectiveness.

Compliance with standards

Compliance with international standards such as ISO/IEC 27001:2022, which provides a framework for the implementation and management of ISMS.

2.7. Cybersecurity legislation in CZ

Act No. 264/2025 Coll.

Act on Cybersecurity (**Cybersecurity Act**), in force since **November 1, 2025**, transposes the **EU NIS2 Directive (EU) 2022/2555** into Czech law and repeals the original Act No. 181/2014 Coll. with its implementing decrees.

- regulates **regulated services** and the obligations of their **providers**,
- defines the terms **cyber security event** and **cyber security incident**,
- establishes **security measures** and two **obligation regimes** (higher / lower),
- sets **registration** and **reporting** duties as well as **inspection** powers of the National Cyber and Information Security Agency (NÚKIB),
- imposes **penalties** for non-compliance (fines up to CZK 250 million or **2 % of the annual global turnover**).

2.8. New implementing decrees

Decree No. 408/2025 Coll.

on **regulated services** - defines which services are regulated and assigns providers to the lower or higher obligation regime.

Decree No. 409/2025 Coll.

on security measures in the **higher obligations regime**.

Decree No. 410/2025 Coll.

on security measures in the **lower obligations regime**.

Decree No. 334/2025 Coll.

on the **NÚKIB Portal** - the official channel for registrations, notifications, and incident reporting.

Cloud computing (public administration)

Decrees No. **411/2025** (security levels of public administration information systems), **412/2025**

(security rules for public administration bodies using cloud services), and **505/2025** (requirements for entry in the cloud computing catalogue, replacing Decree No. 316/2021).

2.9. Key changes under the NIS2 framework

- **self-identification** - each provider itself assesses whether it provides a **regulated service**; the state no longer designates it,
- **registration** - the regulated service must be reported to NÚKIB via the Portal **within 60 days** of meeting the conditions,
- **security measures** - to be implemented **within 12 months** of the registration decision (Decrees No. 409, 410/2025 Coll.),
- **incident reporting** - initial report within **24 hours**, update within **72 hours**, final report within **30 days**,
- **penalties** - up to CZK 250 million or 2 % of the annual global turnover.

2.10. Original framework (repealed on 1 Nov 2025)

Act No. 181/2014 Coll. and Decree No. 82/2018 Coll. ceased to be applicable on October 31, 2025. Documents, policies, and audit reports that still cite them have to be updated to Act No. 264/2025 Coll. and Decrees No. 409 and 410/2025 Coll.; the structure of the measure areas is preserved, the obligation regimes are not.

2.11. Cybersecurity legislation in EU

Directive (EU) 2022/2555 (NIS2)

This directive on measures to ensure a high common level of cybersecurity in the Union was adopted on December 14, 2022. Its aim is to strengthen the capacities of member states in the field of cybersecurity and to introduce measures to manage cybersecurity risks and reporting obligations in critical sectors.

Commission Implementing Regulation (EU) 2024/2690

This regulation, adopted on October 17, 2024, lays down rules for the application of the NIS2 Directive, including technical and methodological requirements for measures to manage cybersecurity risks and clarifies when an incident is considered significant.

2.12. ISMS - Information Security Management System

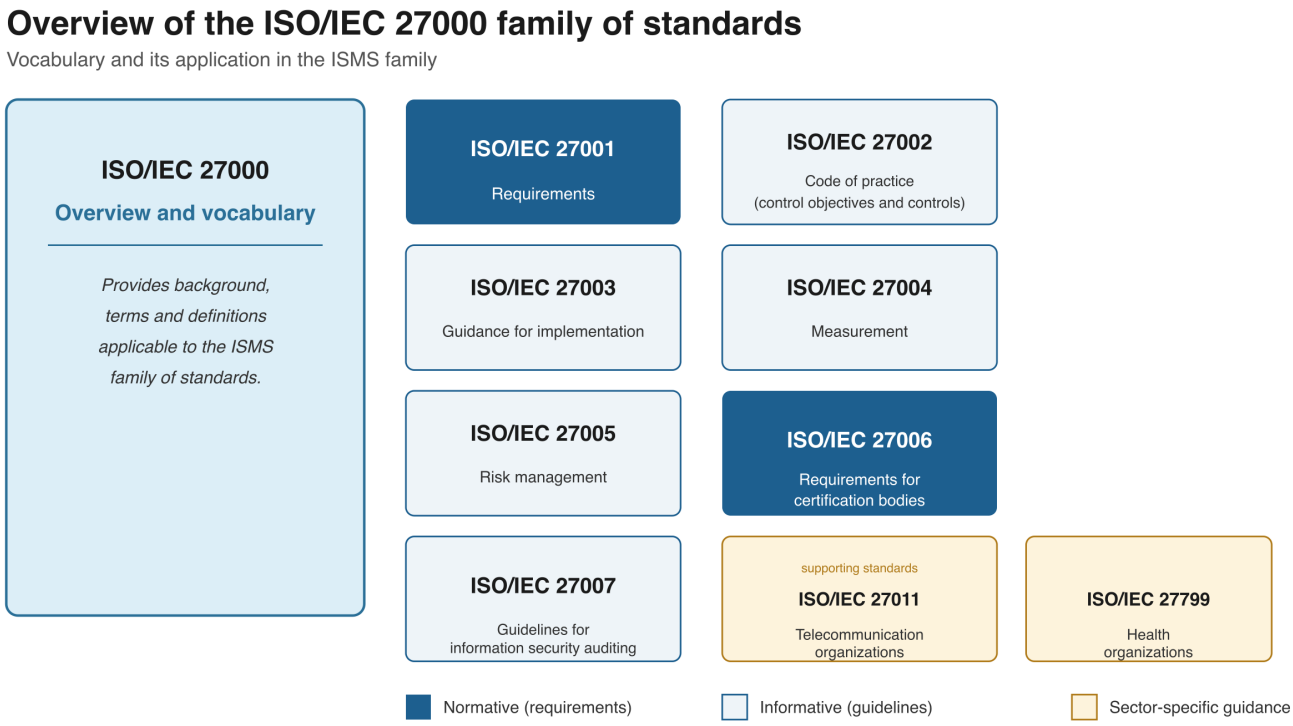
- **ISMS** is an information security solution in IS.
- **ISMS** is a continuous process whose individual activities are repeated.
- **ISMS** is an integral part of a company's information system and overall security system.

ISMS is a documented system in which:

- defined **information assets** are protected,

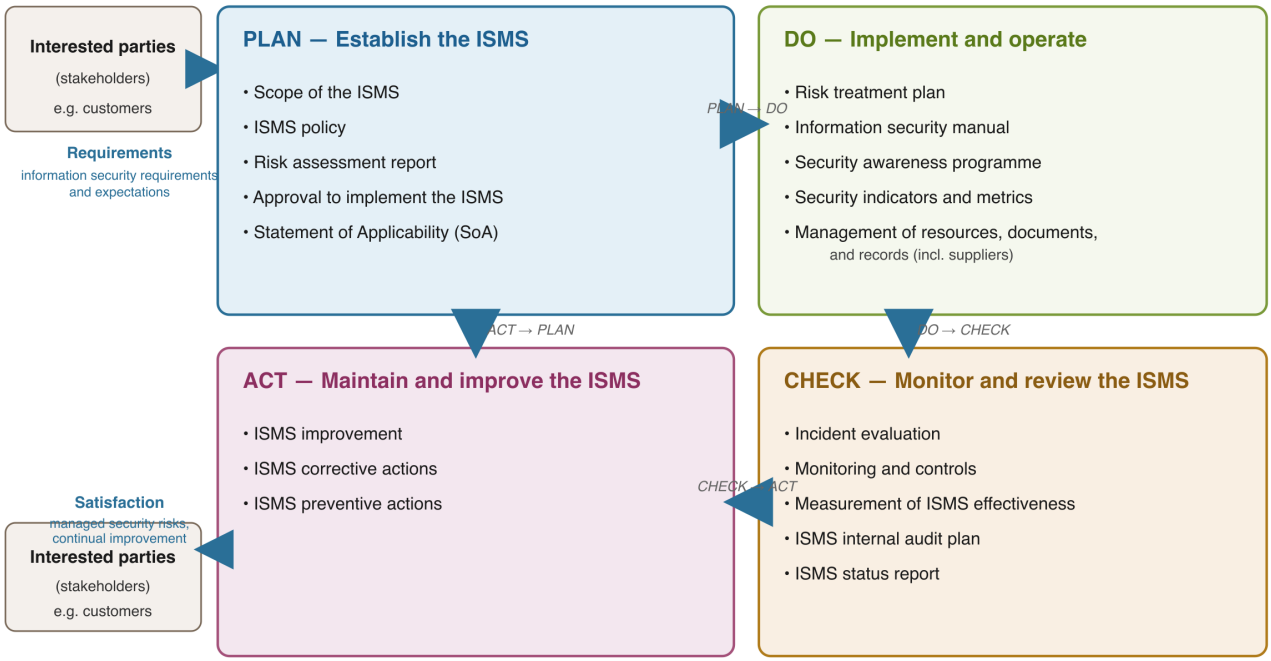
- ◎ information **security risks** are managed,
- 👁 implemented **security measures** are controlled.

ISMS ensures that the security objectives set out in the security policy are achieved through **risk management (RM)**.



2.14. Information security management model [ISO27001]

Process model of the ISMS (ISO/IEC 27001) — PDCA

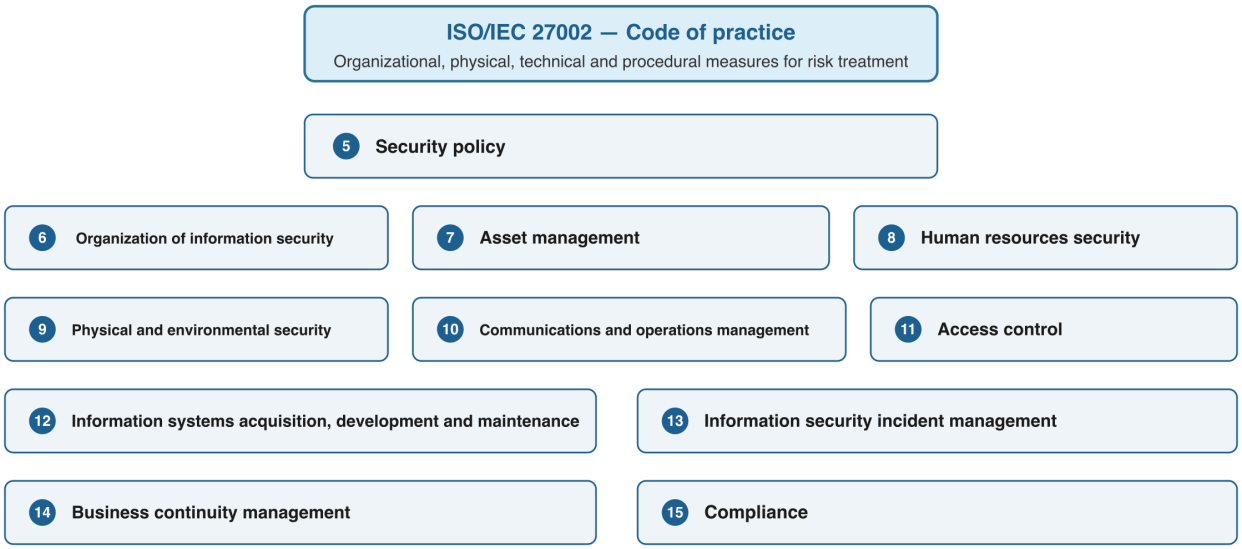


Continual improvement of the ISMS — the cycle (Plan → Do → Check → Act) is repeated over time

2.15. Information security areas [ISO27002]

Information security control objectives and controls

Control domains of ISO/IEC 27002 (clauses of the 2005 edition)



The domain structure is used by ISO/IEC 27001:2005 Annex A and relates to the control areas of the current ISO/IEC 27002:2022.

2.16. Why implement CS?

> The **Cybersecurity Act**, in force since **November 1, 2025**, **requires providers of regulated services** to implement **security measures in**

> **individual areas** in either the **higher** (Decree No. 409/2025 Coll.) or the **lower** (Decree No. 410/2025 Coll.) obligation regime; the individual measure areas are aligned with ISO/IEC 27002:2022.
>
> — Act No. 264/2025 Coll.

2.17. What is cybersecurity implementation?

Organizational measures — **rules and procedures** that protect information and systems:

- identifying, assessing, and managing risks associated with **information assets**,
- procedures for **detecting, reporting, and resolving** security incidents,
- plans to ensure **continuous operation** in the event of a cyber attack or other disruption,
- regular **training** of employees on current threats and security procedures.

2.18. What is cybersecurity implementation? (2)

Technical measures — systems and controls that work on the technical side:

- protection against malware and **unauthorized access**,
- protection of **sensitive information** using **cryptographic algorithms**,
- regular **backup** of important data in case of loss or damage,
- **monitoring and detection** of unusual activity on the network,
- regular **updates** of software and systems to fix **vulnerabilities**.

Chapter 3. Security measures - organizational areas

- Security measures from the **list of security measures** (**Section 14 of Act No. 264/2025 Coll.**) that the **provider of a regulated service** must implement in the **higher** (Decree No. 409/2025 Coll.) or the **lower** (Decree No. 410/2025 Coll.) obligations regime; the areas are aligned with ISO/IEC 27002:2022.

3.1. Management and ISMS

- The **organizational security measures** cover the following areas:
  - Information security management system
  - Top-management requirements
  - Security roles
  - Security policy and security documentation management

3.2. Assets, risks, and suppliers

- Asset management
- Risk management
- Supplier management
- Human resources security

3.3. Operations and change

- Change management
- Acquisition, development, and maintenance
- Access management
- Cybersecurity event and incident management
- Business continuity management
- Cybersecurity audit

Chapter 4. Security measures - technical areas

- The **technical security measures** relate to the following areas (same legal framework, **Act No. 264/2025 Coll.**, **Decrees No. 409 and 410/2025 Coll.**):

4.1. Infrastructure and access

- Physical security
- Communication network security
- Identity management and verification
- Access rights management

4.2. Detection and response

- Detection of cybersecurity events
- Event logging
- Evaluation of cybersecurity events
- Application security

4.3. Cryptography, availability, and special systems

- Cryptographic algorithms
- Ensuring the availability of the regulated service
- Security of industrial, control, and similar specific technical assets

4.4. Measure Areas and Course Modules

The course follows the life cycle of protection; each measure area of the decree is taken up in exactly one module, in the order in which it is decided and implemented. The **organizational** areas:

- ISMS, top management, security roles, policy and documentation management — **§§ 3-6**, **modules 02, 03**
- Asset management, risk management — **§§ 7-8**, **modules 01, 02**
- Supplier management, human resources security — **§§ 9-10**, **module 03**
- Change management, acquisition / development / maintenance, access management — **§§ 11-13**, **module 04**
- Event and incident management, business continuity, cybersecurity audit — **§§ 14-16**, **modules 04, 06**

4.5. Measure Areas and Course Modules (2)

The **technical** areas of the same decree:

- 🔒 Physical security, network security, identity management, access rights management — **§§ 17-20**, **modules 04, 05**
- 👁 Detection, event logging, evaluation of events, application security — **§§ 21-24**, **module 05**
- 🔑 Cryptographic algorithms, availability, industrial and control systems — **§§ 25-27**, **modules 04, 05**

Chapter 5. Cybersecurity Policies

A **set of rules and procedures** that organizations implement to protect their information systems, networks, and data from cyber attacks and other security threats. It includes **technical, administrative, and physical measures** to ensure data security and integrity.

5.1. Cybersecurity Policies (2)

Document	Content
Cybersecurity Policy	**Overall principles** and procedures for protecting information systems and data within a company: rules for access control, data protection, network security, and incident response.
Incident Response Plan	A detailed plan that **describes the steps** to be taken in the event of a cyber attack or security incident: procedures for identifying, reporting, and resolving incidents.
Access Management Policy	Defines **who has access to what** information and systems, and how these accesses are controlled and monitored, including the rules for creating and managing passwords.
Data Backup and Recovery Policy	Establishes procedures for **regular data backup and recovery** in the event of loss or damage, including the rules for storing and encrypting backups.

5.2. Cybersecurity Policies (3)

Document	Content
Training and Awareness Policy	Ensures that employees are **regularly trained** on cyber threats and security procedures: a training plan and programmes to raise awareness of security.
Risk Assessment and Threat Analysis	A document that **identifies and evaluates the risks** associated with the information systems and data, together with the measures to minimize these risks.
Device Management Policy	Establishes rules for the **management and security of all devices** connected to the organizational network, including computers, mobile phones, and other end devices.

5.3. The Systemic Security Policy (SSP)

The **Systemic Security Policy (SSP)** is the **detailed** security policy of the organization. It builds on the overall (fundamental) security policy and on the results of the risk assessment; it is a **dynamic** document that changes with the organization's activities and the technologies used, and it cannot be replaced by generic standards.

The SSP includes

- the **technical component** — a description of the technical solutions and procedures,

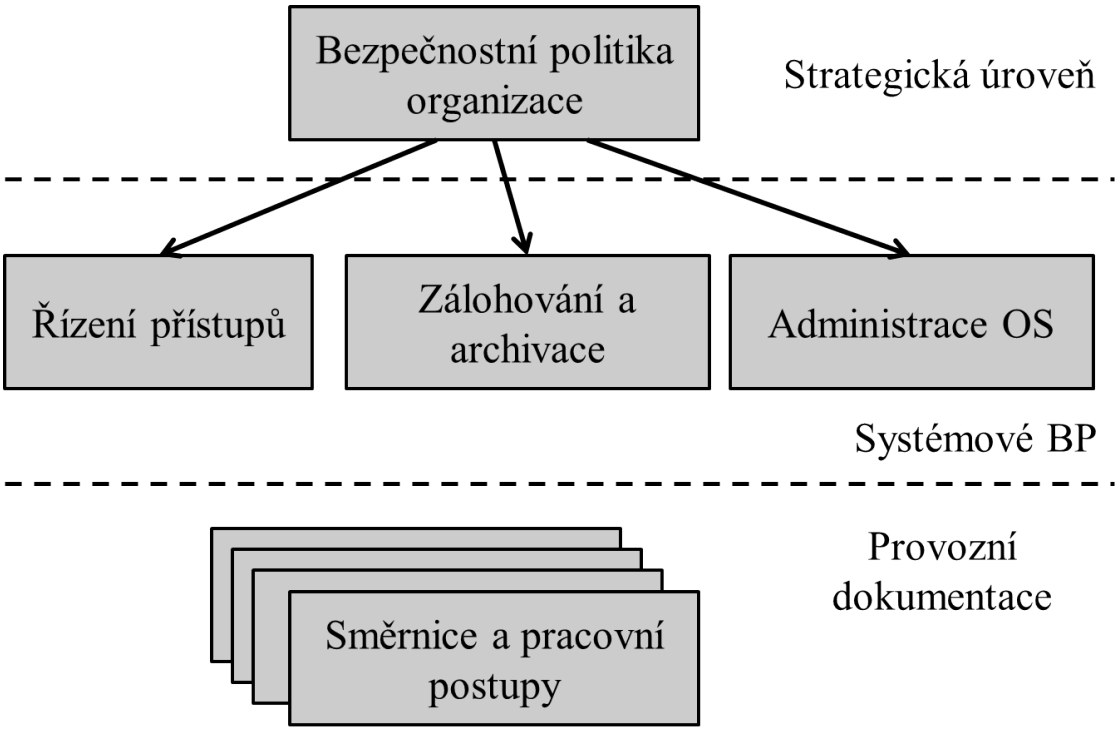
- the **administrative component** — directives and regulations, the definition of powers and responsibilities, the security training plan, etc.

Part of the SSP

- **Monitoring and Audit** — continuous and subsequent monitoring of the effectiveness of the information security system,
- the **Recovery Plan**,
- the **Contingency Plan** (emergency plan).

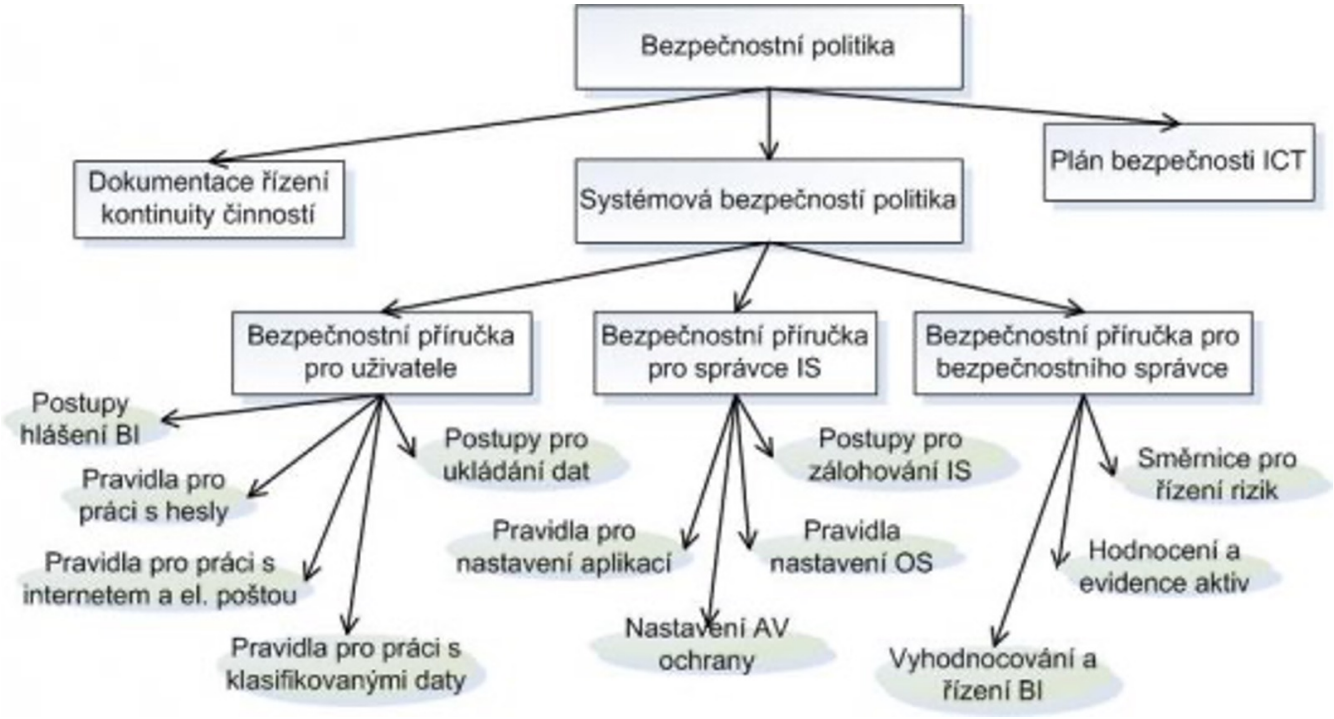
Implementation of the security system is the **realization of the SSP in a specific environment**.

5.4. Structure of the Organization's Security Documentation



The security documentation is organized as a **hierarchy**: the overall security policy and the SSP at the top, followed by the individual security measures and standards, and finally the operational rules, procedures, and records.

5.5. Example of a security document



5.6. Security documentation

- Clear definition of the **duties and responsibilities** of IS users within the organization.

- All employees will be aware of their specific responsibilities and duties when working with the information system.
- Users' security awareness of information security will increase.
- The risk of data leakage, e.g. through email communication etc., will be reduced.
- Limitation of the "absolute power" of administrators and managers.
- Easier to ensure the substitutability of key employees (administrators and managers).

5.7. Emergency plan

- Procedure and response in the event of an accident, failure, or malfunction of the IS
- Part of the **Security Policy**

- IS users should know WHOM to inform and HOW to inform them in the event of a failure

5.8. Summary: Security implementation

- Creation of security **documentation**
- Introduction of security **processes** and **roles**
- Implementation of specific **mechanisms**
- Introduction of security **checks** — **audit**

Chapter 6. Asset Management

- **What do we have?** An **asset inventory** (catalog) of asset types, dependencies, and asset roles — **primary assets** (data, information, services) and the **supporting assets** that make them possible (hardware, software, networks, personnel, locations, organization).
- **How much does it matter? Classification** and **rating** of every asset by **confidentiality, integrity, and availability**. ISO/IEC 27002:2022, control 5.9
- **What do we do with it?** Protection, permitted use, and **disposal** over the whole lifecycle — from acquisition to decommissioning.
- **Why bother?** You cannot protect what you do not know you have, and you cannot prove what you protect without a record of it. The catalog is the input for risk management and for the measures of the following modules.

6.1. Asset Properties

The **CIA triad** — confidentiality, integrity, availability — is defined once, in the previous section of this module; the values assigned to an asset in the classification below are exactly those three dimensions.

6.2. Division of Assets

Primary asset

- is information or a service that is processed or provided by an information and communication system; these primary assets are often value-creating for the functioning of the organization:
  - data,
  - information, and
  - services provided.

Supporting asset

- represents a technical asset, employees, and suppliers involved in the operation, development, administration, or security of an information and communication system.

Tangible supporting assets

Hardware	computers, communication devices, media, specialized technical equipment, etc.
Software	application software, system software, development tools, etc.
Networks	routers, hubs, switches, etc.

Non-tangible supporting assets

Personnel	key employees, administrators, etc.
Location	premises, buildings, rooms, etc.
Organization	governing body, organizational structure, suppliers, etc.

6.3. Asset Identification and Inventory ISO 27002:2022

Asset types

- we can group similar assets and create *asset types*, i.e. assets having similar characteristics, e.g. administrators, users, suppliers, locations, active elements, backup power supplies.

Asset dependencies

- it is necessary to know the relationships between primary and supporting assets; e.g. **several primary assets depend on one supporting asset**.

Asset owner

- the security role responsible for ensuring the development, use, and security of the asset; the roles are detailed in *Asset Roles* below. ISO/IEC 27002:2022, control 5.9

6.4. Asset Roles

Asset Owner	(CZ: *Garant aktiva*) Individual or entity responsible for ensuring that an asset is appropriately protected, used, and managed throughout its lifecycle. ISO/IEC 27002:2022, control 5.9 (responsibility for assets)
Asset Custodian	(CZ: *Správce aktiva*) Person or group entrusted with the day-to-day management, operation, or maintenance of the asset, acting under the instructions of the asset owner. ISO/IEC 27002:2022, section 5 (asset management guidance)
Asset User	(CZ: *Uživatel aktiva*) Authorized individual who uses the asset for business or operational purposes, following security policies and procedures. ISO/IEC 27002:2022, control 5.10

6.5. Asset Ratings

- Asset **inventory** (CZ: *katalog aktiv*)
- Asset **classification** (with **confidentiality**, **integrity**, **availability ratings**)
- Evaluation of the (importance of) **primary assets**

6.6. Availability Rating (Low, Medium)

Low

- *Disruption of asset availability is not important*, and in the event of an outage, a longer period of time (up to approximately **one week**) is normally tolerated for remediation.
- Regular **backups** are sufficient to protect availability.

Medium

- Disruption of asset availability *should not exceed the duration of a* **working day**; a longer outage leads to a *possible threat* to the legitimate interests of the obligated person.

- **Standard backup and recovery** methods are used to protect availability.

6.7. Availability Rating (High, Critical)

High

- Disruption to the availability of the asset *should not exceed* **a few hours**. Any outage must be addressed immediately, as it leads to a *direct threat* to the legitimate interests of the obligated person. The assets are considered to be very important.
- **Backup systems** are used to protect availability, and the restoration of service provision may be subject to operator intervention or the replacement of technical assets.

Critical

- Disruption of asset availability *is not permissible*, and even short-term unavailability (in the order of a **few minutes**) leads to a serious threat to the legitimate interests of the obligated person. Assets are considered critical.
- **Backup systems** are used to protect availability, and service restoration is **short-term and automated**.

6.8. Confidentiality Assessment: Low

Low

- Assets are *publicly accessible* or intended for publication. A breach of asset confidentiality does not jeopardize the legitimate interests of the obligated person.
- When sharing such assets with third parties and using classification according to the traffic light protocol (TLP), the `TLP:WHITE` designation is used. No protection is required.
- Disposal/deletion of assets at the **Low** level

6.9. Confidentiality Assessment: Medium

Medium

- Assets are *not publicly accessible* and constitute the *know-how* of the obligated person; protection of assets is not required by any legal regulation or contractual agreement.
- When *sharing such assets with third parties* and using classifications according to TLP, the designations `TLP:GREEN` or `TLP:AMBER` are mainly used. *Access control measures* are used to protect confidentiality.
- Disposal/deletion of assets at the **Medium** level

6.10. Confidentiality Assessment: High

High

- Assets are not publicly accessible and their *protection is required* by law, other regulations, or contractual agreements (trade secrets, personal data).
- When sharing such assets with third parties and using classification according to TLP, the

`TLP:AMBER` designation is primarily used.

- Measures are used to protect confidentiality, ensuring control and recording of access. Information transfers via communication networks are protected using cryptographic measures.
- Disposal/deletion of assets at the **High** level.

6.11. Confidentiality Assessment: Critical

Critical

- Assets are not publicly accessible and require a *higher level of protection* than the previous category (strategic trade secrets, special categories of personal data).
- When sharing such assets with third parties and using TLP classification, the `TLP:RED` or `TLP:AMBER` designation is primarily used.
- Measures are used to protect confidentiality, ensuring access management and logging. Furthermore, protection methods prevent misuse of assets by administrators. Information transfers are protected using cryptographic means.
- Disposal/deletion of assets at the **Critical** level.

6.12. Asset Catalog

ID	Název	Typ aktiva	Popis	Správce aktiva	Garant aktiva	Hodnota aktiva			
						Dostupnost	Integrita	Důvěrnost	Hodnota aktiva
IC01	Certifikace senzorů	primární	proces certifikace	Odbor certifikace	K. Hovorka	3	4	3	4
IC02	Informace o senzorech	primární	typ senzoru, účel, technické parametry...	Sekce kontroly	S. Reichl	2	3	2	3
IC03	Laboratorní výsledky	primární	výsledné hodnoty z laboratoře	Laboratoř	k. Škuta	2	4	2	4
IC04	Informace o certifikátech	primární	platnost, datum, senzor,...	Odbor certifikace	E. Hejzlar	2	4	1	4
IC05	Kontaktní údaje podavatele	primární	kontaktní osobní údaje,...	Kancelář úřadu	O. Vyhnálek	1	2	1	2
IDB01	Databáze certifikačního systému	podpůrné		Odbor IT	R. Široký	3	4	4	4
IDB02	Databáze webové prezentace	podpůrné		Odbor IT	R. Široký	3	3	3	3
IHW01	Server certifikačního systému	podpůrné		Odbor IT	M. Tichý	3	4	4	4
IHW02	Webový server	podpůrné		Odbor IT	M. Tichý	2	3	3	3
IHW03	Směrovače	podpůrné		Odbor IT	S. Pytlík	3	2	2	3
IHW04	Kabely	podpůrné		Odbor IT	S. Pytlík	3	2	2	3
IHW05	Osobní počítače	podpůrné		Odbor IT	J. Frydrych	2	3	3	3
IHW06	File server	podpůrné		Odbor IT	M. Tichý	3	3	3	3
ILC01	Serverovna	podpůrné		Odbor IT	M. Tichý	4	4	3	4
ILC02	Laboratoř	podpůrné		Laboratoř	k. Škuta	3	4	4	4
ISS01	Dodavatelé laboratorního vybavení	podpůrné		Laboratoř	k. Škuta	3	2	3	3
ISS02	Zaměstnanci laboratoře	podpůrné		Laboratoř	k. Škuta	3	3	4	4
ISS03	Administrátoři	podpůrné		Odbor IT	S. Reichl	3	3	3	3
ISW01	Firewall	podpůrné		Odbor IT	S. Pytlík	3	2	3	3
ISW02	Operační systém	podpůrné		Odbor IT	J. Frydrych	2	2	2	2
ISW03	Certifikační systém	podpůrné		Odbor IT	M. Vodák	3	4	4	4
ISW04	Webová prezentace	podpůrné		Odbor IT	S. Otruba	3	3	2	3

6.13. Assessment of the Importance of Primary Assets

- Scope and importance of **personal data**, **special categories** of personal data, or **trade secrets**,
- Scope of **legal obligations** or other commitments affected,
- Scope of **disruption to internal** management and control activities,
- Damage to public, commercial, or economic interests and possible financial **losses**,

- Impact on the provision of **important services**,
- Extent of **disruption** to normal activities,
- Impact on maintaining **good reputation** or protecting good standing,
- Impact on the **safety and health** of individuals,
- Impact on **international relations**,
- Impact on **users** of the information and communication system.

6.14. Classification of Assets

Asset identification

This includes the identification of all assets that are part of the ISMS, including *data, hardware, software, people, and processes*.

Importance assessment

Each asset is assessed in terms of its *confidentiality*, *integrity*, and *availability*.

Classification assignment

Based on the assessment, assets are classified into different categories according to their importance and sensitivity.

Documentation and review

All classifications are *documented and reviewed* regularly to ensure they remain up to date.

6.15. Asset Disposal Rules

The choice of a disposal method depends on:

- the **value** of the asset (especially in terms of *confidentiality*),
- the **technology** of the asset, types and sizes of information carriers,
- whether the information carrier is **under the control** of the organization or not,
- whether the data is part of a **dedicated or multi-tenant** environment,
- who will perform the **data disposal**,
- availability of **disposal equipment and tools**.

6.16. Asset Disposal Rules (2)

Further criteria for selecting the disposal method:

- **capacity** of the media being disposed of,
- whether **trained personnel** are available,
- **time required** for disposal,
- **cost** of disposal with regard to tools, training, validation, reuse of the information carrier,

- possible **methods** of data disposal,
- **applicable methods** of data disposal with regard to the condition of the information carrier.

6.17. Disposal Levels

The disposal level follows from the asset classification; one classification directly determines the disposal method.

Level	Meaning
Low	No protection required; information is publicly accessible or protection is not required by law. *Removal* suffices.
Medium	Internal know-how; access control and standard backup methods are used to protect the asset. *Overwriting* is the minimum.
High	Protection is required by law, other regulation, or contract (trade secrets, personal data). Access is controlled and logged, transfers are protected cryptographically.
Critical	Higher level of protection than the previous category (strategic trade secrets, special categories of personal data); misuse by administrators must be prevented, so *physical destruction* or verified *cryptographic erasure* is required.

6.18. Disposal: Example

Disposal methods depend on ISO/IEC 27002:2022:

- the information asset **carrier** and
- the disposal **level** (*Low*, *Medium*, *High*, *Critical*)

ISO/IEC 27002:2022 — 7.10 Storage media and 7.14 Secure disposal or re-use of equipment

6.19. Information on Human-readable Media

- **Printed documents**, notes, etc.

  Low

  Removal: Disposal into waste.

  Medium

  Overwriting: Redaction (blacking out). *Physical destruction*: Rendering the information carrier unusable by using a shredding machine.

  High

  Physical destruction: Rendering the information carrier unusable by cross-cut shredding, burning, or chemical decomposition.

Critical

Physical destruction: Rendering the information carrier unusable so that reconstruction is not possible — shredding to particles, or incineration at a temperature that leaves no recoverable residue. A certificate of destruction is retained.

6.20. Mobile Devices

- **Mobile phones**, tablets

Low

Removal: Deletion of information, device reset to factory settings.

Medium

Overwriting: For devices with encrypted storage — deletion of information and reset to factory settings.

High

Physical destruction: Disassembly of the device and destruction of the information storage medium.

Critical

Physical destruction: Disassembly and destruction of the storage medium, combined with **verified cryptographic erasure** — destruction of the device key material (e.g. in the secure element), so that residual memory content is not readable. Destruction is documented by a certificate.

6.21. Network Devices

- **Network devices**; routers, switches, modems
- Office equipment; scanners, printers

Low

Removal: Deletion of information, reset to factory settings.

Medium

Overwriting: Deletion and overwriting with artificial events (e.g. artificial network traffic, test print jobs, etc.).

High

Physical destruction: Disassembly of the device and destruction of the information storage medium.

Critical

Physical destruction: Disassembly and destruction of the storage medium together with non-volatile configuration memory (NVRAM, flash), where credentials, keys, and management consoles may remain after a reset.

6.22. Magnetic Media

- **Magnetic tapes**, floppy disks, hard drives
- **Optical media**: CD, DVD, Blu-ray

Low

Removal: Deletion of data at the file system level.

Medium

Overwriting: Overwriting of data. For encrypted media, secure disposal of cryptographic keys is an alternative.

High

Physical destruction: Destruction of the information carrier.

Critical

Physical destruction: Destruction of the information carrier; where physical destruction is not possible, **degaussing** to erase all magnetic recording, verified by a measuring device.

6.23. Electronic Media

- **Flash memory**

Low

Removal: Deletion of data at the file system level.

Medium

Physical destruction: Destruction of the information carrier.

High

Physical destruction: Destruction of the information carrier.

Critical

Physical destruction: Shredding or incineration of the carrier so that no fragments above the manufacturer's secure-erasure block size survive; where flash is encrypted, secure disposal of the cryptographic keys is the alternative.

6.24. Outsourcing and Cloud

Low

Removal: Deletion of all files, including previous versions. The acceptable method of data disposal should be defined in the contractual agreement.

Medium

Overwriting: Use of encryption at the storage media level and secure disposal of cryptographic keys. The acceptable method of data disposal should be defined in the contractual agreement.

High

Overwriting: Use of encryption at the storage media level and secure disposal of cryptographic keys stored in a certified *Hardware Security Module* (HSM), managed by the customer. At service termination, the master access key is destroyed and the data is overwritten.

Critical

Cryptographic erasure: Encryption at the storage media level with keys held only in a customer-managed HSM; on termination the keys are destroyed first, rendering all remaining copies unreadable. The supplier provides a written certificate of destruction as part of the contractual agreement.