

Implementation of Cybersecurity

Who Manages It

Cyril Klimeš, Tomáš Pitner

Module Contents

1. Module Summary . . . 2
2. Organizational Security and Security Roles . . . 3
   2.1. Activities Required from Organization’s Management . . . 3
   2.2. Activities Required (2) . . . 3
   2.3. Information Security Committee (ICS) . . . 3
   2.4. Information Security Committee (2) . . . 4
   2.5. Composition of ISC . . . 4
   2.6. Members of ISC . . . 4
   2.7. Composition of ISC (2) . . . 5
   2.8. Key activities of ISC . . . 5
   2.9. Main Security Roles . . . 5
   2.10. Role: Cybersecurity Manager . . . 6
   2.11. Differences . . . 6
   2.12. Role: Cybersecurity Architect . . . 6
   2.13. Role: Asset Owner . . . 6
   2.14. Asset Owner (2) . . . 7
3. Role: Cybersecurity Auditor . . . 8
   3.1. Cybersecurity Auditor . . . 8
4. Methodology for a CS Audit . . . 9
5. RACI Matrix . . . 10
   5.1. RACI Matrix . . . 10
6. Cumulation of CS Roles . . . 11
   6.1. Cumulation of CS Roles (2) . . . 11
7. Security and Management Levels of the Organization . . . 12
8. Qualification Requirements for Security Roles . . . 14
   8.1. Qualification Requirements for Security Roles (2) . . . 14
   8.2. Role Substitutability . . . 14
   8.3. Training of Persons Holding Security Roles . . . 14
9. FAQ: Committee and Security Roles . . . 16
10. References . . . 17
11. Supplier Management . . . 18
12. Obligated Entity . . . 19
13. Supplier Management Policy . . . 20
14. Significant Supplier . . . 21
15. Verifiable information provided to the supplier includes . . . 22
16. Steps in the Supplier Management Process . . . 23
17. Document Supplier Management Policy . . . 24
18. Human Resources Security . . . 25

19. Obligated Person 26
20. Security Awareness Development Plan 27
21. Document Security Awareness Development Plan 28
22. User categories according to training requirements 29
23. ICT Access Management 30
24. Human Resources Security Policy Document 31

- Expected lecture date WS 2026: **Oct 20**

Chapter 1. Module Summary

- **Organizational security**: duties of the organization's management, Information Security Committee (composition, members, key activities).
- **Security roles**: cybersecurity manager, cybersecurity architect, asset owner, cybersecurity auditor — duties and differences.
- **Role methodology**: RACI matrix, cumulation of roles, qualification requirements, substitutability, training.
- **Placement in the organization**: management and security levels, where the committee and the roles must sit.
- **Supplier management**: duties of the obligated entity, significant supplier, supplier management policy, process steps, contract clauses.
- **HR security**: security awareness development plan, user categories and training, screening, interface with ICT access management, termination of employment.
- **FAQ**: questions about the committee and about security roles.

Chapter 2. Organizational Security and Security Roles

2.1. Activities Required from Organization's Management

- Ensure **the establishment of a security policy** and **ISMS objectives** compatible with the strategic direction of the organization and the integration of ISMS into all related processes within the organization.
- Ensure **the availability of resources** (e.g., human, financial), inform **employees** about the importance of the ISMS and the importance of achieving compliance with its requirements with all parties concerned.
- Ensure **support** for achieving the intended outputs of the ISMS, lead **employees** to develop the effectiveness of the ISMS and support them in this development.

2.2. Activities Required (2)

- Promote continuous **improvement** of the ISMS.
- Support personnel holding **security roles** in promoting cyber security in their areas of responsibility.
- Ensure **the establishment of rules** for determining administrators and personnel who hold security roles and ensure that confidence of administrators and persons holding security roles is maintained.
- For persons holding security roles, **ensure appropriate powers** and **resources**, including budgetary resources, to fulfill their roles and perform related tasks.
- Ensure **testing of business continuity plans**, **recovery**, and processes related to the management of **cybersecurity incidents**.

2.3. Information Security Committee (ICS)

- **Information Security Committee** a.k.a. *Cybersecurity Committee*
- ISMS does not enforce the existence of an ISC; its role is implied from the ISO 27000 standards — *need for an ISMS* ISO 27001:2022, *management structures* ISO 27002:2022)
- In the **lower** regime no committee is required; only a **person responsible for cybersecurity** (CZ: *osoba pověřená kybernetickou bezpečností*) must be designated Decree 410/2025 Coll.
- Under Act 264/2025 Coll. (Cyber Security Act), the committee — *Výbor pro řízení kybernetické bezpečnosti* — is **required** in the **higher** regime Decree 409/2025 Coll., § 4(3):
  - established by **senior management**, which designates its members,
  - composed of persons with **appropriate powers and professional competence**,

- must include **at least one senior-management representative** (or a person authorized by them) **and the cybersecurity manager**,
- must convene **at least once a year**, and a **record** of each meeting must be produced.

2.4. Information Security Committee (2)

> ISC is composed of persons with the appropriate powers and professional competence for the overall management and development of the information security management system and persons significantly involved in the management and coordination of activities related to cybersecurity, of which at least one member must be a representative of senior management or a person authorized by them and a cybersecurity manager.

2.5. Composition of ISC

Under **Act 264/2025 Coll.**, in the **higher obligations regime** the **senior management** designates persons for the security roles Decree 409/2025 Coll., § 4(4):

- **Cybersecurity Manager** — responsible for the proper functioning of the ISMS.
- **Cybersecurity Architect** — responsible for providing a secure architecture of the ICT system.
- **Asset Custodian** (CZ: *garant aktiva*) — responsible for the development, use, and security of the asset.
- **Cybersecurity Auditor** — responsible for conducting impartial cybersecurity audits. **Substitutability** must be ensured at least for the **manager** and the **architect** Decree 409/2025 Coll., § 4(5). In the **lower obligations regime** only a **person responsible for cybersecurity** needs to be designated Decree 410/2025 Coll.

2.6. Members of ISC

Committee Chair

This person should be a senior figure in the organization, such as the *Chief Information Security Officer* (CISO) or CEO or managing director, or their deputy.

Cybersecurity Managers

Persons responsible for the day-to-day administration and implementation of security policies and procedures.

Chief Financial Officer or Financial Analyst

A person who provides a financial perspective and analyzes the costs associated with cybersecurity.

IT and IT Security Personnel

Technicians and IT security experts who have technical knowledge and experience in implementing and managing security measures.

2.7. Composition of ISC (2)

Legal and compliance professionals

Legal and compliance experts who ensure that the organization **complies** with all relevant **laws and regulations**.

Communications and PR professionals

Individuals who ensure transparent **communication** with internal and external stakeholders about **security measures and incidents**.

Human resources

HR specialists who ensure that all employees are properly **trained in cybersecurity**.

2.8. Key activities of ISC

Responsibility

for the **overall management and development** of cyber security within the obligated entity.

Creation

of a cybersecurity **framework, direction, and principles** for the obligated entity's cybersecurity (defining strategic goals and direction for development in the area of cybersecurity).

Definition of roles

and **responsibilities** within the ISMS.

Definition of requirements

for **reporting and auditing** the ISMS.

Auditing the current state

of cybersecurity within the obligated entity and determining whether planned objectives are being met.

2.9. Main Security Roles

Statutory security roles under **Act 264/2025 Coll.** in the **higher obligations regime** Decree 409/2025 Coll., § 4(4): Cybersecurity Manager:: ensures the proper functioning of the ISMS. Cybersecurity Architect:: ensures the design and implementation of security measures to ensure the secure architecture of the information and communication system. Cybersecurity Auditor:: is responsible for conducting cyber security audits. Asset Owner:: is responsible for ensuring the development, use, and security of assets.

2.10. Role: Cybersecurity Manager

- Responsible for **ISMS**: this is a **key role**, ensuring the proper functioning of **ISMS**.
- Responsible for informing senior management about activities arising from the scope of his/her responsibilities and the status of ISMS.
- The aim is to facilitate the implementation of the ISMS concept and to ensure that senior management is well informed and involved in cyber security issues.

2.11. Differences

Cybersecurity Manager

- **Responsible** for managing the ISMS
- Proposes, coordinates
- "**Central brain**" of ISMS
- Therefore, **must not** be responsible for ICT operations!

Senior management

- Responsible for **managing the organization**
- Ensures **approval and implementation** of security measures through other employees of the organization

2.12. Role: Cybersecurity Architect

- Responsible for ensuring the design and implementation of security measures to guarrantee security of the information and communication system **architecture**, eg., security at the application level.
- A knowledgeable and experienced person: there may be more than one person.

2.13. Role: Asset Owner

Responsible for security of the Asset:

Expertise and experience

Persons with in-depth knowledge of specific assets, whether IT systems, financial data, or other key resources. They should have experience in managing and protecting them.

Clearly defined roles and responsibilities

Each owner should have a **clearly defined role** and responsibility for certain assets. This includes the obligation to monitor, evaluate, and report on the status of assets.

Communication skills

Effective **communication** is key to sharing information about risks, incidents, and changes related to the assets in question.

2.14. Asset Owner (2)

Cooperation with other departments

Owners should **cooperate** with other departments, such as IT, security, compliance, and finance, to ensure a consistent and comprehensive approach to asset management.

Regular training

Owners should be regularly **trained** on the latest procedures and technologies.

Chapter 3. Role: Cybersecurity Auditor

Cybersecurity Auditor verifies the functioning of information security management systems in the organization.

Audit planning and preparation

Collaborates with cybersecurity managers to plan the audit, including setting audit objectives and scope.

Evaluation of security measures

Evaluates current security measures and their compliance with requirements and standards.

3.1. Cybersecurity Auditor

Providing feedback

Provides independent feedback on the effectiveness of cybersecurity systems and recommendations for improvement.

Documentation of results

Processes audit conclusions and documentation of results, including identification of risks and recommendations for their resolution.

Monitoring of implementation of recommendations

Monitors the implementation of recommendations from the audit and assessment of their effectiveness.

Chapter 4. Methodology for a CS Audit

- Position of the **auditor**, including the auditor's *Code of Ethics*
- Outputs: audit implementation plan and reports
- Storage of audit documentation

- audit **objectives**, **subject** of the audit,
- audit **criteria**,
- identification of the **audit team** and persons who participated in the audit,
- **date and place** where audit activities were performed,
- audit **findings**, including deficiencies identified during review and evaluation of the subject of the audit w.r.t.established control criteria,
- audit **conclusions**, including the auditor's opinion in relation to the audited area.

Chapter 5. RACI Matrix

The Matrix maps CS **Processes** to CS **Roles** (people) who are:

R - Responsible
: odpovědný

A - Accountable
: zodpovědný

C - Consulted
: konzultovaný

I - Informed
: informovaný

IS/CS Role	Committee	Manager	Architect	Auditor	Asset Owner
Overall management and development	A	R	R	-	C
ISMS	A	R	C	-	C
Proposing security measures	C	A	R	-	C
Implementation of measures	C	A	R	-	C
Ensure assets development, use and security	-	A	C	-	R
Audit	I	C	C	A/R	C

Chapter 6. Cumulation of CS Roles

- Is it possible for security roles in relation to a specific system to be performed by the same employee? Generally prohibited if a conflict of interest may arise.

Under the current legislation, **Act 264/2025 Coll.** and Decree 409/2025 Coll. (higher obligations regime), it is expressly *prohibited* to:

- entrust the **cybersecurity manager** with roles responsible for the **operation of a system** — the manager must not be entrusted with roles responsible for the operation of technical assets of the regulated service § 5(1),
- entrust the **cybersecurity auditor** with **any other security role** (to guarantee the impartiality of the audit § 5(4)); however, the auditor may be a member of the ISCommittee, as this is not a security role.

6.1. Cumulation of CS Roles (2)

- Combining the roles of **manager, architect, and asset custodian** in a single person is **explicitly permitted**; only the **substitutability** of the manager and the architect must still be ensured § 4(5).
- If the merger of specific roles is not prohibited by the legislation, it is possible to merge roles, although this cannot be recommended based on best practice procedures.

- Supporting material of the National Cyber and Information Security Agency (NÚKIB)
- Source version 3.1, valid as of December 22, 2022; legal references updated to Act No. 264/2025 Coll.



This material describes one possible option of how to implement the security roles required by the Cybersecurity Decree into the organizational structure. It serves as a supporting guideline and does not replace any laws or implementing regulations.

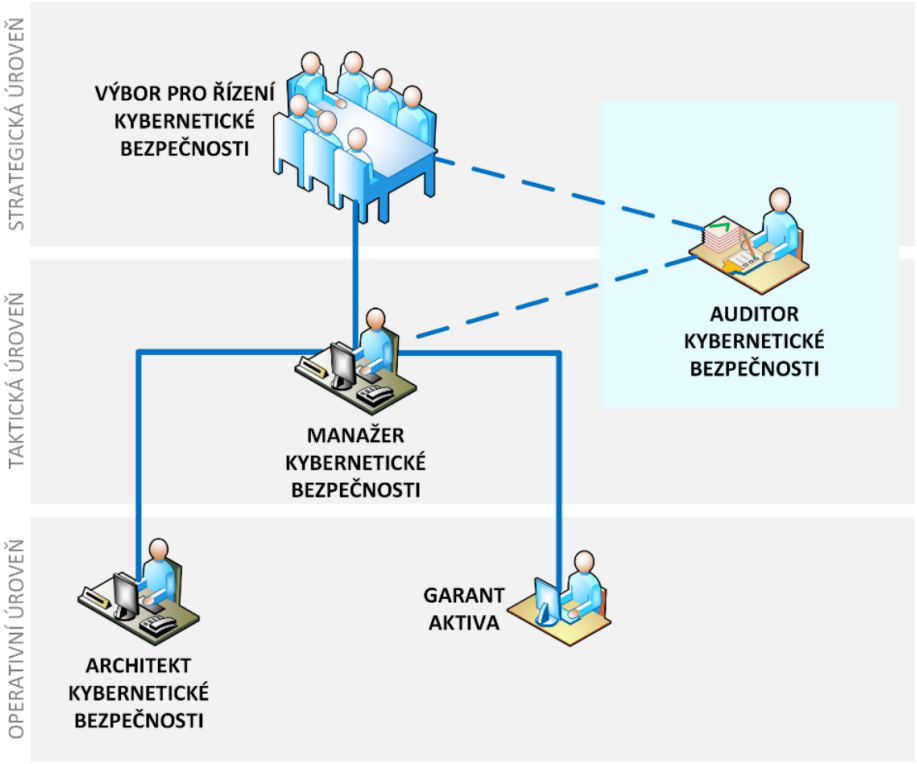
Chapter 7. Security and Management Levels of the Organization

Ideally, the Cyber/ICT Security Department should be placed under ICT Governance, which is directly managed by the top management of the organization. Its purpose is, simply put, to maximize organizational efficiency using ICT tools.

It is especially necessary to remember that cyber/ICT security cuts across all levels of management. Therefore, roles should be established that will ensure security at individual levels of management.

Level	Expected security activity
Top management	Establishes the security policy and the security measures, provides resources, and is accountable for the overall security of the regulated service.
ICT Governance	Coordinates the security agenda across departments and resolves conflicts between security and business objectives.
Cyber/ICT Security Department	Operates the security measures: identity and access management, recording of events, incident management, monitoring of compliance.
ICT Operations	Runs the systems; must remain **separated** from the Cyber/ICT Security Department so that those who implement the measures do not also control them.

Hierarchii výboru kybernetické bezpečnosti a bezpečnostních rolí je možno v rámci úrovní managementu organizace znázornit následovně



Obrázek č. 2: Hierarchie výboru kybernetické bezpečnosti a bezpečnostních rolí

Figure 1:Hierarchy of cybersecurity committee and roles

Chapter 8. Qualification Requirements for Security Roles

Where the previous section described *who* holds the roles, this section describes *who may* hold them. The qualification requirements are set by Decree No. 409/2025 Coll., Section 5. The earlier NÚKIB supporting material (v3.1, 2022) also allowed a shortened practice with a university degree; the decree no longer permits it — **at least 3 years** is required in all three cases.

Cybersecurity Manager

Person responsible for the ISMS; must be trained and prove professional competence through at least **3 years of practice** in managing cybersecurity or information security. Reports regularly to top management. The role must be **separated from the operation of technical assets**.

Cybersecurity Architect

Designs and ensures implementation of security measures and a secure system architecture. Requires at least **3 years of experience** in designing and implementing security measures.

8.1. Qualification Requirements for Security Roles (2)

Cybersecurity Auditor

Conducts cybersecurity audits, **independent from other roles** (must not hold any other security role). Requires at least **3 years of experience** in conducting cybersecurity or ISMS audits.

Asset Custodian

Person appointed by the organization responsible for development, use, and protection of an asset (confidentiality, availability, integrity). Equivalent to "asset owner" in ISO/IEC 27000.

Decree No. 409/2025 Coll., Section 4 (senior management requirements) and Section 5 (security roles); Act No. 264/2025 Coll., Section 14

8.2. Role Substitutability

- Substitutability must be ensured for the **Cybersecurity Manager** and the **Cybersecurity Architect**.
- Appointed substitutes do not require mandatory practice.
- Appointed persons must be given adequate **authority and resources**.

Decree No. 409/2025 Coll., Section 4

8.3. Training of Persons Holding Security Roles

Within human resource security, professional training of persons holding security roles must be ensured in accordance with the security awareness development plan (introductory and regular training).

Decree No. 409/2025 Coll., Section 10 (human resources security)

Chapter 9. FAQ: Committee and Security Roles

Can external experts be appointed? Yes, but risks must be managed.

What certifications should roles have? The supporting material recommends:

- **Manager**: CISM, CRISC, CISSP, BI Manager (ČIA)
- **Architect**: CEH, CompTIA Security+, CISM, CRISC, CISSP, BI Manager
- **Auditor**: CISA, CIA, CRISC, Lead Auditor ISMS, BI Auditor

Can one person hold multiple roles? Yes, but the **auditor** must always be independent.

Is the committee required in both obligations regimes? In the **higher** regime the committee and the roles are explicitly required. In the **lower** regime (Decree No. 410/2025 Coll.) no committee is required, only a **person responsible for cybersecurity**.

Chapter 10. References

- Act No. 264/2025 Coll., Cybersecurity Act
- Decree No. 409/2025 Coll. — security measures in the higher obligations regime
- Decree No. 410/2025 Coll. — security measures in the lower obligations regime
- ČSN ISO/IEC 27000, 27001, 27002

For questions, please contact the Secretariat of the National Cyber and Information Security Agency (NÚKIB): regulace@nukib.cz

Chapter 11. Supplier Management

Chapter 12. Obligated Entity

1. establishes **rules for suppliers** that take into account the requirements of the information security management system,
2. **keeps records** of its significant suppliers,
3. **demonstrably informs** its significant suppliers in writing about their recording
4. familiarizes its suppliers with the rules and **requires compliance** with these rules,

1. **manages risks** associated with suppliers,
2. in connection with the management of risks associated with significant suppliers, ensures that contracts concluded with significant suppliers contain relevant areas
3. regularly reviews the performance of contracts with significant suppliers from the perspective of the information security management system

Chapter 13. Supplier Management Policy

- Rules and principles for **selecting** suppliers,
- rules for **assessing risks** related to suppliers,
- **contract requirements** for service levels and methods and levels of implementation of security measures and for determining mutual contractual liability,
- rules for **conducting checks** on the implementation of security measures,
- rules for **evaluating** suppliers.

Chapter 14. Significant Supplier

It has a key role for secure operation:

- **operator** of an information or communication system,
- and anyone who **enters into a legal relationship** with the obligated entity that is significant in terms of the security of the information and communication system.
- **Operators** are a subset of significant suppliers – **ensuring the functionality** of ICT

Chapter 15. Verifiable information provided to the supplier includes

- Identification of the **administrator or operator**,
- identification of the **information system**,
- identification of the **significant supplier**,
- notification of the fact that the supplier is a **significant supplier** for the controller and, where applicable, that the significant supplier is also the operator,
- content of **security rules** for suppliers taking into account the requirements of ISMS.

Chapter 16. Steps in the Supplier Management Process

- Establish **rules** for suppliers,
- register **significant suppliers** (and demonstrably inform them of this fact),
- **manage risks** related to supplier relationships –– take into account risks from pre-contractual analyses when selecting provisions for contracts and subsequently take into account risks in the summary risk analysis. Suppliers must be recorded as supporting assets and the risks associated with them must be addressed,
- regularly review whether the established rules are being followed –– one possible input for the review is the results of customer audits.

Chapter 17. Document Supplier Management Policy

- Rules and principles for selecting **suppliers**
- Rules for assessing supplier risks: Identification of risks arising from access by external entities
- Requirements for *Agreements on Service Level, Methods and Levels of Implementation of Security Measures and Determination of Mutual Contractual Liability*:
  - Security requirements for access by external entities
  - Security requirements in agreements with external entities
  - Security measures for contractual relationships with significant suppliers
- Rules for **checking** the implementation of security measures
- Rules for **evaluating suppliers**

Chapter 18. Human Resources Security

Chapter 19. Obligated Person

- establishes a **security awareness** development plan aimed at ensuring adequate **training** and improvement of security awareness
- ensures that **users, administrators, persons** holding security roles, and **suppliers are instructed** on their obligations and security policy through initial and regular training
- for persons holding security roles in accordance with the security awareness development plan, it shall ensure regular **professional training**
- it shall ensure the **monitoring of compliance** with the security policy by users, administrators, and persons holding security roles,
- in the event of **termination** of the contractual relationship with administrators and persons holding security roles, ensure the **transfer of responsibilities**,
- Determine **rules and procedures** for dealing with cases of **violation** of established security rules by users, administrators, and persons holding security roles.

Chapter 20. Security Awareness Development Plan

- **Content and dates** of training for users, administrators, and persons holding security roles,
- Content and dates of **training for new employees**,
- Identification of **significant suppliers**,
- Overviews containing the subject matter of individual training courses and a **list of persons** who have completed the training,
- Forms and methods of **evaluating the plan**.

Chapter 21. Document Security Awareness Development Plan

Affected employees

RACI (competence) matrix (Responsible, Accountable, Consulted, and Informed)

Persons responsible for implementing individual activities

Security training

- Initial training
- Regular training
- Specialized training

Effectiveness assessment

Chapter 22. User categories according to training requirements

- regular users – basic,
- administrators – advanced/specialized
- …….

Chapter 23. ICT Access Management

Human resources security interfaces with **ICT access management**: the access rights of a person follow from the person's position, and they must be revoked or changed when the position or the classification changes, and revoked upon termination of the contractual relationship.

- access based on **groups and roles**, with access rights, permissions, and a unique identifier,
- **limits** on privileged permissions — to the level necessary for the performance of work duties,
- **limits and controls** on software tools capable of bypassing system or application controls,
- regular **reviews** of the settings of all access rights,
- use of an **identity management and verification tool** and an access rights management tool,
- **documentation** of the assignment and revocation of access rights.

The full list of obligations for access rights management is in the fourth module, under *Access Control*.

Chapter 24. Human Resources Security Policy Document

Roles and Responsibilities

Employee Screening

Rules for Developing Security Awareness and Methods of Evaluating It

- Methods and forms of instruction for users, asset guarantors, administrators, and other persons holding security roles

Information security training

Breach of work duties and disciplinary proceedings

Responsibilities upon termination of employment

- Revocation of access rights
- Responsibilities upon termination of the basic employment relationship
- Return of loaned resources