

Implementation of Cybersecurity

How We Verify It Works

Cyril Klimeš, Tomáš Pitner

Module Contents

1. Module Summary . . . 2
2. Cybersecurity Audit . . . 3
   2.1. ISMS Audit . . . 3
   2.2. Main steps of a Cybersecurity Audit . . . 3
   2.3. Main steps (2) . . . 3
   2.4. Main steps (3) . . . 4
   2.5. The Cybersecurity Auditor is responsible for . . . 4
   2.6. Written Audit Report . . . 4
   2.7. Written Audit Report (2) . . . 4
   2.8. Audit Intervals . . . 5
3. Example: Audit of an Organization . . . 6
   3.1. Organizational measures . . . 6
   3.2. Technical controls . . . 13
4. Vulnerability Management and Penetration Testing . . . 19
5. Vulnerability Management . . . 20
   5.1. Scanning or Penetration Testing . . . 20
6. Penetration Testing . . . 21
7. Reporting an Actively Exploited Vulnerability . . . 22
8. Roles in Vulnerability Management . . . 23
   8.1. Vulnerability Record . . . 23
9. Digital Forensics . . . 24
10. Forensic Process . . . 25
   10.1. Standards and Frameworks . . . 25
   10.2. Roles in Digital Forensics . . . 25
   10.3. Evidence and Chain of Custody . . . 26
   10.4. Evidence Collection and Acquisition . . . 26
   10.5. Order of Volatility . . . 26
   10.6. Tools and Techniques . . . 27
   10.7. Forensic Readiness . . . 27
11. GAP Analysis . . . 28
   11.1. Areas of Analysis . . . 28
12. GAP Analysis Process . . . 29
   12.1. GAP Analysis Contents . . . 29
13. Example GAP Analysis . . . 31
   13.1. Example Action Plan . . . 31
   13.2. Measuring Success . . . 31
   13.3. Frequency and Continuous Monitoring . . . 32
14. Gap Analysis Report . . . 33

14.1. Report Structure 33
14.2. Example: Gap Analysis Report 33

- Expected lecture date WS 2026: **Dec 15**

Chapter 1. Module Summary

- **Cybersecurity audit**: the scope covers the *entire* implemented security measures and the information security management system — management system, organizational measures, technical measures.
- **Cybersecurity auditor**: plans audits, evaluates compliance with requirements, policies, and standards, documents the process, evaluates findings, reports, and checks effectiveness.
- **Main steps**: audit criteria and objectives, scope, audit team, checklist, conducting the audit, analysis of results, implementation of measures, control and monitoring.
- **Vulnerability management**: scanning (at least yearly), penetration testing (at least every 2 years, whole scope within 5 years), re-testing, the CRA reporting timeline, roles, and the vulnerability record.
- **Written audit report**: findings, risks arising from the findings, recommendations with a responsible addressee, conclusions.
- **Audit intervals**: at least every **2 years**, after a **significant change**, or in systematic units covering the whole scope within **5 years**.
- **Digital forensics**: the forensic process, order of volatility, roles, chain of custody, forensic readiness.
- **GAP analysis**: areas of analysis, the process, contents, an example analysis, action plan, measuring success, continuous monitoring.
- **Outcome**: a prioritized action plan closing the gap between the required and the actually implemented measures.

Chapter 2. Cybersecurity Audit

Act No. 264/2025 Coll., Section 14 (list of security measures); Decree No. 409/2025 Coll., Section 16 (cybersecurity audit) and Section 5(4) (cybersecurity auditor role)

2.1. ISMS Audit

The audit covers the **entire scope of the implemented security measures and the information security management system**: the management system, the organizational measures, and the technical measures.

Example: audit of an organization

- Criteria used for the audit and the evidence collected
- Verbal description of findings + evidence

See *Example: Audit of an Organization* at the end of this module for a complete audit aid covering the control points of the decree.

2.2. Main steps of a Cybersecurity Audit

Establishing audit criteria and objectives

The first step is to define the audit criteria, which involves determining the standards and requirements against which the security system will be evaluated. This may include internal policies, industry standards (e.g., ISO/IEC 27001:2022), and legislative requirements.

Determining the scope of the audit

Determining which parts of the IT infrastructure and processes will be included in the audit. This may include servers, network devices, applications, databases, and user accounts.

Creating a team of auditors

Assembling a team of experts to conduct the audit. This team may include both internal staff and external consultants specializing in cybersecurity.

2.3. Main steps (2)

Compiling a checklist

Creating a detailed list of control points that will be evaluated during the audit. This list includes specific security measures and procedures that need to be verified.

Conducting the audit

The actual audit involves *collecting data*, *interviewing* key employees, *reviewing* documentation, and *testing* security measures. This may include penetration testing, vulnerability scanning, and log analysis.

Analysis of results

Once the audit is complete, the collected data is analyzed and evaluated. Weaknesses and

vulnerabilities that may pose security risks are identified.

2.4. Main steps (3)

Implementation of measures

Based on the audit results, security measures are designed and implemented to eliminate identified vulnerabilities and improve the overall level of security.

Control and monitoring

After the measures have been implemented, it is important to regularly monitor and control their effectiveness. This includes repeated audits and ongoing monitoring of security measures.

2.5. The Cybersecurity Auditor is responsible for

- planning control activities and audits in the area of cybersecurity,
- evaluating the degree of compliance of the information security management system and implemented security measures with defined requirements, established security policies, and appropriate security standards,
- maintaining documentation on the audit process in accordance with established methodologies,
- evaluating the collected audit findings and comparing them with audit criteria,
- communicating audit results and proposing recommendations,
- preparing final audit reports,
- checking the effectiveness of the measures taken

2.6. Written Audit Report

Findings from the audit, including in particular negative results of processes, i.e., deficiencies identified during the review and evaluation of the findings in comparison with objectively established control criteria,

Risks arising from the findings, including the impact on the audited area,

2.7. Written Audit Report (2)

Recommendations for eliminating the identified deficiencies and improving the quality of the cybersecurity system and preventing or mitigating identified risks — recommendations should be described in an understandable manner, must have a specific addressee responsible for implementing the recommendations, and the costs of implementing the recommendations should be proportionate to the risk arising from the findings.

Conclusions containing the auditor's opinion on the audited area, positive and negative findings.

2.8. Audit Intervals

Decree No. 409/2025 Coll., Section 16

- At least every **2 years**
- In the event of a **significant change**
- Can be implemented in **systematic units** — the entire scope of the audited areas is covered once within **5 years**

Audit under Decree No. 409/2025 Coll., Section 16 (working English translation)

(1) The obliged entity shall draw up a plan for carrying out the cybersecurity audit.

(2) In the cybersecurity audit the obliged entity a) assesses whether the security measures required by the Act and this Decree have been implemented, b) assesses the conformity of the implemented security measures with legal regulations, internal regulations, contractual obligations, and best practice, and c) carries out and documents an audit of compliance with the rules and procedures laid down in the security policy, including a review of technical conformity and of previously laid-down corrective measures referred to in paragraph (3)(b).

(3) The obliged entity a) incorporates the results of the cybersecurity audit referred to in paragraph (2) into the security awareness development plan and into risk management, and b) lays down, on the basis of the result of the cybersecurity audit referred to in paragraph (2), any corrective measures to be taken without undue delay.

(4) The cybersecurity audit referred to in paragraph (2) is carried out a) in the event of significant changes, within their scope, b) at regular intervals of at least once every **2 years**, and c) in accordance with the cybersecurity audit plan.

(5) Where, in justified cases, it is not possible to carry out the audit in its full scope referred to in paragraph (2) within the period referred to in paragraph (4)(b), the cybersecurity audit may be carried out continuously in systematic units, so that the full scope of the audit referred to in paragraph (2) is covered at least once every **5 years**.

(6) The cybersecurity audit shall be carried out by a person meeting the conditions laid down in Section 5(4), who independently assesses the correctness and effectiveness of the implemented security measures.

Source: Decree No. 409/2025 Coll., Section 16 (own working translation).

Chapter 3. Example: Audit of an Organization



The audit aid below was issued under Act No. 181/2014 Coll. and Decree No. 82/2018 Coll., which ceased to be effective on 1 November 2025. Since then, Act No. 264/2025 Coll., on Cyber Security, and its implementing decrees No. 409/2025 Coll. (higher regime of obligations) and No. 410/2025 Coll. (lower regime of obligations) apply. The list of security controls and its structure have remained essentially the same, so the aid may continue to be used with reference to these current regulations.

The audit verifies the security controls laid down by the decree. The control points are grouped into the **information security management system and organizational measures** (§ 3--§ 16) and the **technical controls** (§ 17--§ 29). Each control point is assessed and the finding is recorded together with the evidence.

3.1. Organizational measures

§ 3 Information security management system

a) defines, taking into account the requirements of interested parties and organizational security, the scope of the information security management system, within which it identifies the organizational units and assets covered by the information security management system,

b) defines the objectives of the information security management system,

c) for the defined scope of the information security management system

d) manages risks,

e) establishes and approves the information security policy for the information security management system,

f) ensures that a cyber security audit is performed

g) ensures regular evaluation of the effectiveness of the information security management system

h) continuously identifies and subsequently manages significant changes

1. updates the information security management system

j) manages the operation and resources of the information security management system.

§ 4 Asset management

a) defines a methodology for asset identification,

b) defines a methodology for asset valuation

c) identifies and records assets,

d) designates and records asset owners,

e) classifies and records primary assets in terms of confidentiality, integrity, and availability

f) identifies and records the relationships between primary and supporting assets and assesses the implications of dependencies between primary and supporting assets,

g) evaluates supporting assets, taking into account in particular their mutual dependencies

h) based on the asset valuation, sets up and introduces the protection rules necessary to secure the individual asset levels,

1. defines the acceptable ways of using assets and the rules for handling assets with regard to their level, including rules for the secure electronic sharing and physical transfer of assets,

j) determines the method of disposing of data, operational records, information and their copies, or of disposing of technical data media

§ 5 Risk management

a) defines a methodology for asset valuation, including the definition of risk acceptability criteria,

b) identifies relevant threats and vulnerabilities;

c) performs risk assessment at regular intervals

d) takes relevant threats and vulnerabilities into account in the risk assessment and evaluates the potential impact on assets

e) prepares a risk assessment report

f) prepares a statement of applicability based on the security requirements and the results of the risk assessment

g) prepares and implements a risk treatment plan

h) takes significant changes, changes to the scope of the information security management system, controls, and cyber security incidents into account in the risk assessment and in the risk treatment plan

1. implements security controls in accordance with the risk treatment plan.

§ 6 Organizational security

ensures the establishment of the information security policy and information security management system objectives, and designates the person who will hold the security role:

a) cybersecurity manager,

b) cybersecurity architect,

c) asset owner and

d) cyber security auditor.

The Cyber Security Management Committee is composed of persons with the relevant authority and professional competence for the overall management and development of the information security management system, and of persons significantly involved in the management and coordination of activities related to cybersecurity; it must include at least one representative of top management or a person appointed by them, and the cybersecurity manager.

§ 7 Security roles

The cybersecurity manager is the security role responsible for the information security management system; the performance of this role may be entrusted to a person who is trained for this activity and demonstrates professional competence through practice in cybersecurity management or information security management.

The cybersecurity architect is the security role responsible for ensuring the design of the implementation of security controls so as to guarantee a secure architecture of the information and communication system; the performance of this role may be entrusted to a person who is trained for this activity and demonstrates professional competence through practice in designing the implementation of security controls and ensuring security architecture.

The asset owner is the security role responsible for ensuring the development, use, and security of the asset.

The cyber security auditor is the security role responsible for performing the cyber security audit; the performance of this role may be entrusted to a person who is trained for this activity and demonstrates professional competence through practice in conducting cyber security audits or information security management system audits.

§ 8 Supplier management

a) defines supplier rules that take into account the requirements of the information security management system,

b) keeps a record of its significant suppliers,

c) demonstrably informs its significant suppliers in writing of their entry in the record

d) informs its suppliers of the rules and requires compliance with these rules,

e) manages risks associated with suppliers,

f) in connection with managing risks associated with significant suppliers, ensures that contracts concluded with significant suppliers contain the relevant areas

g) regularly reviews compliance with contracts with significant suppliers from the perspective of the information security management system

§ 9 Personnel security

a) taking into account the state and needs of the information security management system, establishes a security awareness development plan aimed at ensuring appropriate education and the improvement of security awareness, which specifies the form, content, and extent of instructing users, administrators, persons holding security roles, and suppliers on their obligations and on the information security policy, as well as the theoretical and practical training required for users, administrators, and persons holding security roles,

b) designates the persons responsible for carrying out the individual activities listed in the plan,

c) in accordance with the security awareness development plan, ensures that users, administrators, persons holding security roles, and suppliers are instructed on their obligations and on the information security policy through induction and regular training,

d) for persons holding security roles, in accordance with the security awareness development plan, ensures regular professional training, based on the current cybersecurity needs of the obligated person,

e) in accordance with the security awareness development plan, ensures regular training and verification of employees' security awareness in line with their job responsibilities,

f) ensures monitoring of compliance with the information security policy by users, administrators, and persons holding security roles,

g) in the event of termination of a contractual relationship with administrators or persons holding security roles, ensures the handover of responsibilities,

h) evaluates the effectiveness of the security awareness development plan, the training carried out, and other activities related to improving security awareness

1. defines rules and procedures for handling breaches of established security rules by users, administrators, and persons holding security roles.

§ 10 Operational security and communications

a) the rights and obligations of administrators, users, and persons holding security roles,

b) procedures for starting up and shutting down the system, for restarting or resuming system operation after a failure, and for handling error states or exceptional conditions,

c) procedures for monitoring cyber security events and controls to protect access to records of these events,

d) rules and procedures for malware protection,

e) technical vulnerability management,

f) contact details of the persons responsible for providing system and technical support,

g) procedures for managing and approving operational changes,

h) procedures for monitoring, planning, and managing human and technical resource capacity,

1. rules and procedures for protecting information and data throughout their entire life cycle,

j) rules and procedures for the installation of technical assets,

k) the performance of regular backups and verification of the usability of the backups made

l) rules and procedures for ensuring the security of network services.

§ 11 Change management

a) reviews the potential impact of changes and

b) identifies significant changes.

In addition, for significant changes the obligated person

a) documents their management,

b) performs a risk analysis,

c) takes measures to mitigate all adverse impacts associated with significant changes,

d) updates the information security policy and information security documentation,

e) ensures their testing

f) ensures the possibility of rollback to the original state.

§ 12 Access control

a) controls access based on groups and roles,

b) assigns to each user and administrator accessing the information and communication system access rights and permissions and a unique identifier,

c) manages the identifiers, access rights, and permissions of applications and technical accounts,

d) introduces security controls for managing device access to the resources of the information and communication system,

e) introduces the security controls necessary for the secure use of mobile devices and other technical devices, and, where applicable, also security controls related to the use of technical devices not under the obligated person’s administration,

f) restricts the assignment of privileged permissions to the level strictly necessary for performing job duties,

g) restricts and controls the use of software tools that may be capable of circumventing system or application controls,

h) grants and revokes access rights in accordance with the access control policy,

1. performs regular reviews of the settings of all access rights, including the assignment to access groups and roles,

j) uses the identity management and authentication tool as an access rights management tool

k) enforces compliance by users with the established procedures when using private authentication information,

l) ensures the revocation or modification of access rights upon a change of position or assignment of users, administrators, or persons holding security roles,

m) ensures the revocation or modification of access rights upon termination or change of a contractual relationship

n) documents the granting and revoking of access rights.

§ 13 Acquisitions, development and maintenance

a) manages risks in accordance with this Decree

b) manages significant changes in accordance with this Decree

c) defines security requirements,

d) incorporates security requirements into the acquisition, development, and maintenance project,

e) ensures the security of the development and testing environment and protects the test data used,

f) performs security testing of significant changes before they are put into operation

g) fulfils the requirement of § 19(3) if the purpose of the acquisition or development is an identity management and authentication tool.

§ 14 Cyber security event and incident management

a) establishes a process for the detection and assessment of cyber security events and the management of cyber security incidents,

b) assigns responsibilities and defines procedures for the detection and assessment of cyber security events and incidents and for the coordination and management of cyber security incidents,

c) defines and applies procedures for the identification, collection, acquisition, and retention of reliable evidence needed for the analysis of a cyber security incident,

d) ensures the detection of cyber security events,

e) upon the detection of cyber security events, further complies with § 22 and 23,

f) ensures that users, administrators, persons holding security roles, other employees, and

suppliers report unusual behavior of the information and communication system and any suspected vulnerabilities,

g) ensures the assessment of cyber security events, in the course of which a decision must be made as to whether they are to be classified as cyber security incidents

h) ensures the management of cyber security incidents in accordance with the established procedures,

1. takes measures to avert and mitigate the impact of a cyber security incident,

j) reports cyber security incidents in accordance with § 32,

k) keeps records of cyber security incidents and their management,

l) investigates and determines the causes of the cyber security incident and

m) evaluates the effectiveness of the cyber security incident resolution and, based on that evaluation, determines the necessary security controls or updates the existing security controls to prevent the recurrence of the cyber security incident in question.

§ 15 Business continuity management

a) the rights and obligations of asset owners, administrators, and persons holding security roles,

b) using risk assessment and impact analysis, evaluates and documents the potential impact of cyber security incidents and assesses the potential risks associated with a threat to business continuity,

c) sets business continuity management objectives by determining

1. the minimum level of services provided that is acceptable for the use, operation, and administration of the information system of a critical information infrastructure, the communication system of a critical information infrastructure, or a significant information system,
2. the recovery time within which, after a cyber security incident, the minimum level of services provided by the information system of a critical information infrastructure, the communication system of a critical information infrastructure, or a significant information system will be restored, and
3. the data recovery time as the deadline by which data will be restored after a cyber security incident, and

d) the business continuity management policy,

e) prepares, updates, and regularly tests business continuity plans and disaster recovery plans related to the operation of the information and communication system and related services and

f) implements measures to increase the resilience of the information and communication system against cyber security incidents and availability limitations

§ 16 Cyber security audit

a) performs and documents an audit of compliance with the information security policy, including a review of technical conformity, and takes the audit results into account in the security awareness development plan and the risk treatment plan

b) assesses the conformity of security controls with best practice, legal regulations, internal regulations, other regulations, and contractual obligations relating to the information and communication system, and determines any corrective actions needed to ensure compliance.

3.2. Technical controls

The technical controls are laid down in § 17--§ 29:

- § 17 Physical security
- § 18 Communications security
- § 19 Identity management and authentication
- § 20 Access rights management
- § 21 Malware protection
- § 22 Logging of events of the information and communication system, its users and administrators
- § 23 Cyber security event detection
- § 24 Collection and assessment of cyber security events
- § 25 Application security
- § 26 Cryptographic controls
- § 27 Ensuring the level of information availability
- § 28 Industrial, control and similar specific systems
- § 29 Digital services

§ 17 Physical security

a) prevents damage, theft, or misuse of assets or interruption of the services provided by the information and communication system,

b) establishes a physical security perimeter delimiting the area in which information is stored and processed and the technical assets of the information and communication system are located,

c) for the physical security perimeter established under letter b), takes the necessary measures and applies physical security means to prevent unauthorized entry, to prevent damage and unauthorized interference, and to ensure protection at the facility level and within facilities.

Physical security means are in particular

a) mechanical barriers,

b) electrical intrusion alarm devices,

c) means limiting the effects of fires,

d) means limiting the effects of natural disasters,

e) access control systems,

f) camera systems,

g) devices ensuring protection against power supply failure

h) devices ensuring optimal operating conditions.

§ 18 Communications security

a) ensures the segmentation of the communication network,

b) ensures the control of communication within the communication network and at the communication network perimeter,

c) uses cryptography to ensure the confidentiality and integrity of data during remote access, remote administration, or access to the communication network using wireless technologies,

d) actively blocks unwanted communication and

e) for network segmentation and the control of communication between its segments, uses a tool that protects the integrity of the communication network.

§ 19 Identity management and authentication

A user identity verification tool that uses password-only authentication ensures

a) identity verification before activities are started in the information and communication system,

b) control of the number of possible failed login attempts,

c) resistance of stored or transmitted authentication data to unauthorized theft and misuse,

d) storage of authentication data in a form resistant to offline attacks,

e) re-verification of identity after a specified period of inactivity,

f) preservation of the confidentiality of authentication data during access restoration and

g) centralized identity management.

For verifying the identity of users, administrators, and applications, it uses an authentication mechanism that is not based solely on the use of an account identifier and password, but on multi-factor authentication with at least two different types of factors.

§ 19 Identity management and authentication (password rules)

Until the requirement of the preceding paragraph is met, the tool for verifying the identity of users, administrators, and applications must use authentication based on cryptographic keys and guarantee an equivalent level of security.

Until the requirements of the preceding paragraphs are met, a tool for verifying the identity of users, administrators, and applications that uses an account identifier and password for authentication must:

- enforce password length rules of at least **12 characters for users** and **17 characters for administrators and applications**,
- allow the entry of a password of at least **64 characters**,
- impose **no restrictions** on the use of upper- and lower-case letters, digits, and special characters,
- allow users to change their password, with an interval of at least **30 minutes** between two password changes,
- prevent users and administrators from selecting the most frequently used passwords, creating passwords based on repeatedly recurring characters, the login name, the e-mail address, the system name, or similar means, and reusing previously used passwords, with a memory of at least **12 previous passwords**, and
- require a mandatory password change at intervals of no more than **18 months**, whereby this rule does not apply to accounts used for system recovery in the event of a disaster.

§ 20 Access rights management

permission management

a) for access to individual applications and data and

b) for reading data, writing data, and changing permissions.

§ 21 Malware protection

a) taking into account the importance of assets, ensures the use of a tool for continuous automatic protection of

1. endpoints,
2. mobile devices,
3. servers,
4. data storage and removable data media,
5. the communication network and communication network components and
6. similar devices,

b) monitors and controls the use of removable devices and data media,

c) controls the automatic execution of content from removable devices and data media,

d) controls permissions for code execution and

e) performs regular and effective updates of the malware protection tool.

§ 22 Logging of events of the information and communication system, its users and administrators

ensures

a) unique network identification of the originating device if a tool that changes its network identification is used in the communication network,

b) the collection of information on security and operational events; in particular, it records

1. date and time including the time zone specification,
2. the type of activity,
3. the identification of the technical asset that recorded the activity,
4. the unique identification of the account under which the activity was performed,
5. the unique network identification of the originating device and
6. the success or failure of the activity,

c) the protection of the information obtained against unauthorized reading and any modification,

d) the recording of

1. sign-in and sign-out to all accounts, including failed attempts,
2. activities performed by administrators,
3. successful and unsuccessful manipulation of accounts, permissions, and rights,
4. activities not performed due to a lack of access rights and permissions,
5. user activities that may affect the security of the information and communication system,
6. the start and end of technical asset activities,
7. critical and error messages of technical assets and
8. accesses to event records, attempts to manipulate event records, and changes to the settings of logging tools and

e) the synchronization of a unified time for technical assets at least once every 24 hours.

§ 23 Cyber security event detection

ensures the detection of cyber security events appropriately with regard to the importance of assets within

a) endpoints,

b) mobile devices,

c) servers,

d) data storage and removable data media,

e) active network components and

f) similar assets.

It further ensures

a) verification and control of data transmitted within the communication network and between communication networks,

b) verification and control of data transmitted at the communication network perimeter and

c) blocking of unwanted communication.

§ 24 Collection and assessment of cyber security events

a) the collection and assessment of events recorded under § 22 and 23,

b) the searching and grouping of related records,

c) providing information to designated security roles about detected cyber security events,

d) assessing cyber security events for the purpose of identifying cyber security incidents, including the timely warning of designated security roles,

e) limiting cases of incorrect event assessment through regular updates of the rules for assessing cyber security events and timely warning

f) using the information obtained by the cyber security event collection and assessment tool to optimally configure the security controls of the information and communication system.

§ 25 Application security

performs penetration tests of the information and communication system focusing on important assets, namely

a) before they are put into operation and

b) in connection with a significant change.

§ 26 Cryptographic controls

a) uses currently resilient cryptographic algorithms and cryptographic keys,

b) uses a key and certificate management system that

1. ensures the generation, distribution, storage, modification, validity restriction, and revocation

of certificates and the disposal of keys and

2. allows for control and audit,

c) enforces the secure handling of cryptographic controls and

d) takes into account the recommendations on cryptographic controls issued by the Agency and published on its website.

§ 27 Ensuring the level of information availability

a) the availability of the information and communication system for achieving the objectives under § 15,

b) the resilience of the information and communication system to cyber security incidents that could reduce its availability,

c) the availability of important technical assets of the information and communication system and

d) the redundancy of assets necessary to ensure the availability of the information and communication system.

§ 28 Industrial, control and similar specific systems

a) the use of technical and software means intended for a specific environment,

b) the restriction of physical access to the devices of these systems and to the communication network,

c) the segregation of the communication network intended for these systems from the rest of the infrastructure,

d) the restriction and control of remote access to these systems,

e) the protection of individual technical assets of these systems against the exploitation of known vulnerabilities and

f) the restoration of the operation of these systems after a cyber security incident.

§ 29 Digital services



The provision of § 29 (digital services) originates from the repealed Act No. 181/2014 Coll. and follows the NIS1 Directive (EU) 2016/1148; under Act No. 264/2025 Coll. this category has been abolished and such services are now covered as regulated services under the NIS2 regime.

- implements security controls in accordance with Commission Implementing Regulation (EU) 2018/151 of 30 January 2018
- reports contact details
- reports cyber security incidents

Chapter 4. Vulnerability Management and Penetration Testing

Act No. 264/2025 Coll., Section 14 (list of security measures); Decree No. 409/2025 Coll., Section 24 (application security); Regulation (EU) 2024/2847 (Cyber Resilience Act)

Testing closes the loop of the course: it **verifies** that the measures implemented in the previous module actually work and finds what they miss. The application security methods that are used during development are described in *Application Security* in the previous module.

Chapter 5. Vulnerability Management

Scan

Scan the technical assets regularly, from both the internal and the external communication network, at least once a year, and feed the results into risk management. Decree No. 409/2025 Coll., Section 24(4)

Plan testing

Use penetration testing with regard to the asset and risk evaluation: from the internal and external networks, before commissioning, and in connection with a significant change; regularly at least every two years, with the whole scope covered within five years. Record the date and the persons who perform it. Decree No. 409/2025 Coll., Section 24(5)

Assess

Triage each finding by severity (four levels — see *Detection of Cybersecurity Events* in the previous module) and by the classification of the affected asset.

Remediate

Apply fixes, patches, or compensating measures by priority; assets whose support ended or that cannot be patched are registered and protected by measures of an equivalent or higher level. Decree No. 409/2025 Coll., Section 24(1), (2)

Re-test

Re-test every finding to verify that the measure works. Decree No. 409/2025 Coll., Section 24(6)

Record

Record the finding, the decision, the fix, and the re-test result as evidence for the audit.

5.1. Scanning or Penetration Testing

Criterion	Vulnerability scanning	Penetration testing
Nature	Automated tools compare known vulnerabilities and missing patches against the assets	A person creatively attacks the system, chains weaknesses, and may use social engineering
Goal	Find the known weaknesses everywhere	Prove what is actually exploitable and measure the real impact
Scope	All technical assets, inside and outside	Risk-based: the critical assets and those affected by a significant change
Frequency	At least once a year Decree No. 409/2025 Coll., Section 24(4)	At least every two years; the whole scope within five years Decree No. 409/2025 Coll., Section 24(5)
Output	A list of findings with a severity	A report with the exploited paths, the impact, and remediation advice

Chapter 6. Penetration Testing

A penetration test is bounded by a written mandate: the **scope**, the **rules of engagement**, the time window, and the **authorised testers**, whose names and the date are recorded for the audit. Decree No. 409/2025 Coll., Section 24(5)

Reconnaissance

Gather information about the target from public sources and from the internal network.

Scanning

Identify the reachable services and the potential entry points.

Exploitation

Attempt to exploit the weaknesses without harming production.

Post-exploitation

Determine how far the tester can get and what the impact would be.

Reporting

Hand over the findings with the reproduction steps, the severity, and the recommendations.

Chapter 7. Reporting an Actively Exploited Vulnerability

Manufacturers of products with digital elements report an actively exploited vulnerability as a phased notification: an **early warning within 24 hours** of becoming aware, a **notification within 72 hours**, and a **final report within 14 days** after a corrective measure is available. Regulation (EU) 2024/2847 (Cyber Resilience Act), Article 14

Chapter 8. Roles in Vulnerability Management

Role	Responsibility
Asset owner	Owns the affected asset and accepts or approves the residual risk.
Tester or analyst	Runs the scans and the penetration tests and writes the findings.
Security officer	Sets the scanning and testing cadence, the triage thresholds, and the exceptions, and follows the CRA reporting duties.
Operations and patch manager	Rolls out the fixes and updates and keeps the unsupported-asset register.
Auditor	Verifies the evidence: the scan and test reports and the re-test results — see *Cybersecurity Audit* in this module.

8.1. Vulnerability Record

Table 1. Template: vulnerability record (skeleton)

Item	Content
Identification	ID and the date the finding was discovered.
Discovery source	Vulnerability scan, penetration test, incident, or a report from outside.
Affected asset and version	The technical asset, the application, and the affected version.
Description	The nature of the vulnerability and how it can be exploited.
Severity and impact	Severity on the four-level scale and the business impact on the asset.
Decision	Fix, accept, or compensate, with the reason and the approver.
Fix and owner	The measure and the person responsible for it.
Deadline	The date by which the measure must be in place.
Re-test result	The outcome of the verification, with the date and the tester. Decree No. 409/2025 Coll., Section 24(6)
Status and evidence	Open or closed, with links to the scan, test, and re-test records.

Chapter 9. Digital Forensics

Act No. 264/2025 Coll., Section 14 (handling cybersecurity events and incidents); Decree No. 409/2025 Coll., Section 22 (event recording)

Digital forensics is the process of identifying, collecting, acquiring, preserving, and analyzing digital evidence in a way that makes it usable in an incident investigation and, if necessary, in legal proceedings. It answers *what happened, when, how, and who was involved.*

The obligated person defines and applies procedures for the identification, collection, acquisition, and retention of reliable evidence needed for the analysis of a cyber security incident. Digital forensics is triggered by a cyber security incident and supports the incident management process (*Managing Cybersecurity Events and Incidents*, earlier in this module). Digital forensics reconstructs **what happened** after an incident, in a way that holds up as evidence. It is the investigative counterpart of the audit: the audit checks whether the measures work, forensics checks the trace the attacker left behind. ---

Chapter 10. Forensic Process

Identification

Recognise that an incident has occurred and decide which evidence is needed.

Preservation

Secure the evidence before it changes: isolate the system, start a chain-of-custody record, and hash every item.

Acquisition

Copy the volatile and the non-volatile data (memory, disk, logs) with a write blocker, so that the original is not altered.

Analysis

Reconstruct the timeline, find the entry point and the actions of the attacker, and correlate the events recorded by *Recording Events* in the previous module.

Reporting

Write a factual report: what was found and how it was obtained; separate the facts from the interpretation.

Retention

Keep the evidence and the report for the retention period (the event records for at least 18 months) and hand them to the authorities or the insurer when required.

10.1. Standards and Frameworks

ISO/IEC 27037

Guidelines for the identification, collection, acquisition, and preservation of digital evidence.

ISO/IEC 27042

Guidelines for the analysis and interpretation of digital evidence.

NIST SP 800-86

Guide to Integrating Forensic Techniques into Incident Response — the practical process model.

10.2. Roles in Digital Forensics

Role	Responsibility
Incident responder	Recognises the incident first and secures the scene before anything changes.
Forensic analyst	Acquires and analyses the evidence and writes the report.
Security officer	Coordinates with the authorities and decides on disclosure.

Role	Responsibility
Data protection officer	Assesses the personal-data impact of the evidence and of any disclosure. GDPR, Regulation (EU) 2016/679
Management	Owns the remediation and the communication decisions.
External provider	Performs the analysis under contract when the in-house capability is missing — see *Supplier Management* in the third module.

10.3. Evidence and Chain of Custody

Table 2. Template: evidence and chain-of-custody record (skeleton)

Item	Content
Case and incident	The case ID and the incident the evidence belongs to.
Evidence item	The item and its unique ID (disk, image, memory dump, log export).
Source	The system, the location, and the owner of the item.
Acquisition	The date, the method, and the tool category used to obtain the copy.
Hash	The hash value and the algorithm, to prove that the copy is unchanged.
Storage	Where the item and its copy are kept and who has access.
Custody transfers	From whom to whom, when, and why — the chain of custody.
Analysis and result	Who analysed it and what the analysis concluded.
Retention and disposal	How long it is kept and how it is destroyed afterwards.

10.4. Evidence Collection and Acquisition

Source	Evidence
Memory	Running processes, open network connections, injected code, encryption keys.
Disk	File system metadata, deleted files, artifacts, application data; acquired as a **forensic image** through a write blocker.
Logs	System, application, and security logs; records of events under § 22; SIEM data.
Network	Captured traffic, flow records, DNS and proxy logs.
Mobile and removable media	Messages, location data, documents, and data on removable data media.

10.5. Order of Volatility

Collect the most volatile evidence first, because it disappears fastest.

Order	Evidence	Why it is volatile
1	CPU registers and cache	Overwritten immediately.
2	Memory (RAM)	Lost on power-off; holds the keys, the sessions, and the running malicious code.
3	Network connections and temporary files	Close or are overwritten within seconds.
4	Disk and file system	Persists, but changes with every use.
5	Logs and monitoring data	Rotate and are overwritten — see *Recording Events* in the previous module.
6	Backups and archives	The most stable; needed for recovery and for long-term evidence.

10.6. Tools and Techniques

- **Forensic imaging** — bit-for-bit copies with hash verification.
- **Write blockers** — prevent modification of the original media.
- **Timeline analysis** — order events from multiple sources.
- **File system and artifact analysis** — recover deleted data and usage traces.
- **Memory forensics** — analyze the memory of a live system.
- **Network forensics** — analyze captured traffic and flow data.

10.7. Forensic Readiness

Forensics succeeds only if it was prepared for: keep and synchronise the event records required by Section 22, retain them for at least 18 months, pre-approve an external forensic provider, and give the responders the authority to isolate a system immediately. Decree No. 409/2025 Coll., Section 22(5), (6)

Chapter 11. GAP Analysis

A **GAP analysis** compares the **current state** of the organization with a **desired state** defined by a standard or by law, and produces a prioritized list of gaps together with an action plan.

Its scope follows the scope of the cybersecurity audit (*Cybersecurity Audit*, earlier in this module), and its result is the input to the audit findings and to the corrective measures.

11.1. Areas of Analysis

Area	What is examined
Use of computing technology and configuration of communication technologies	Evaluation of how computing resources are utilized, assessment of communication systems and configurations.
Information security in information systems and technological assessments	Review of measures protecting data, evaluation of IT infrastructure, network components, and security measures.
Physical security and personnel security	Assessment of physical measures protecting facilities and equipment, review of personnel-related security measures.
Documentation of security procedures and their actual implementation, process audits	Comparison of documented security protocols against actual practice; examination of internal processes, policies, and guidelines.
Human factor assessment and compliance with legislation	Verification of employee training and awareness; analysis of legal documents and obligations.

Chapter 12. GAP Analysis Process

Step	Activity	Result
1. Defining objectives and scope	Determine the objective (e.g., improving cybersecurity), the areas to be included, and which standards or regulations serve as the reference framework (e.g., ISO/IEC 27001:2022, NIS2).	Scope and reference framework.
2. Information gathering	Collect documentation and data about current security measures and processes. Interview key staff to gain their perspective on the current state.	Evidence of the current state.
3. Current state analysis	Compare the current state with the requirements of the selected standard or regulation. Identify areas where the organization meets the requirements and areas where there are deficiencies.	Compliance matrix.
4. Gap identification and root cause analysis	Document specific deficiencies, classify them by severity, and identify why they exist and how they can be addressed.	Prioritized list of gaps.
5. Action plan development	Propose concrete steps and measures to eliminate the identified deficiencies. Assign responsibility and set timelines for each step.	Action plan.
6. Presentation of results	Prepare a report with the results and the action plan, and present the results to the organization's management to secure their support for implementation.	Management decision.
7. Implementation and measuring results	Execute the plan, track progress, measure outcomes against the desired state, and gather feedback on the effectiveness of the implemented measures.	Measured improvement.

12.1. GAP Analysis Contents

Column	Content
Cybersecurity area	The area or process being analyzed.
Current state	What is implemented today, with evidence.
Desired state	What the standard or law requires.
Identified gaps	The difference between the two, classified by severity.
Action steps	The measure proposed to close the gap.

Column	Content
Responsibility and deadline	Who implements the measure, and by when.

Chapter 13. Example GAP Analysis

Objective and scope

Improve data protection and access control.

Information gathering

Current state — encryption not implemented, passwords only. Desired state — all data encrypted, multi-factor authentication (MFA) in place.

Gap identification

Identified gaps — missing encryption software, no MFA solution.

Root cause analysis

Lack of investment in encryption technologies, insufficient awareness of MFA benefits.

Action plan and evaluation

Implement encryption software, deploy MFA, train staff; measure the number of security incidents, incident response times, and gather employee feedback.

13.1. Example Action Plan

Goal	Steps	Responsibility	Timeline
Improving data protection	Implement encryption software for all data storage; train employees on the importance and correct use of encryption tools; regularly review and update encryption keys.	IT Department	3 months
Improving access control	Select and deploy an appropriate MFA solution; update access policies and procedures; train employees in MFA use.	Security Team	2 months
Improving incident response	Develop a detailed incident response plan; conduct simulations and exercises to test the plan; update the plan based on exercise results.	Incident Response Team	4 months
Increasing cybersecurity awareness	Organize regular training sessions and workshops; create and distribute informational materials; conduct regular phishing tests and evaluate employee responses.	HR Department with IT	Ongoing

13.2. Measuring Success

Indicator	What it shows
Number of security incidents and incident response time	Whether the treatment actually reduces incidents and shortens their handling.
Number of successful phishing attacks	The effect of awareness measures, measured by phishing tests.
Audits, penetration testing, and incident simulations	Whether the implemented measures work as designed and the team can react.
Compliance with standards and benchmarking	Progress against the selected standard (e.g., ISO/IEC 27001:2022, NIS2) and against peers in the industry.

13.3. Frequency and Continuous Monitoring

Recommended frequency

Annually for most organizations. Also after major organizational changes, new technology adoption, legislative changes, or significant incidents.

Regular audits

Internal and external.

Penetration testing

Regular vulnerability testing.

Employee training

Ongoing awareness-building activities.

Result measurement

Compare outcomes with the desired state after implementation.

Feedback

Gather stakeholder feedback on the effectiveness of measures.

Continuous improvement

Repeat the analysis periodically to ensure ongoing compliance.

Chapter 14. Gap Analysis Report

The **Gap analysis report** is the outgoing document of the whole process — it is what is handed to management under step 6 *Presentation of results*. It must be structured so that the reader can follow the reasoning from the reference framework to the proposed measures and their monitoring.

14.1. Report Structure

Section	What it contains
1. Introduction	Purpose of the report and scope of the analysis (which cybersecurity areas were covered).
2. Methodology	The procedure followed and the standards or regulations used as the reference framework (e.g., ISO/IEC 27001:2022, NIS2, Act No. 264/2025 Coll., CRA, DORA).
3. Current state	Overview of the currently implemented controls and processes, and an assessment of how they meet the requirements.
4. Identified gaps	List of gaps between the current and target state, classified by severity and impact on the organization.
5. Cause analysis	Root causes of the identified gaps and why they exist.
6. Proposed measures	Specific action steps to close the gaps, with their prioritization.
7. Timeline	Schedule, key milestones, and deadlines for completing the individual steps.
8. Responsibilities	Who is responsible for each measure; roles and tasks of the individual team members.
9. Monitoring and assessment	How the effectiveness of the measures will be measured (KPIs, regular audits) and how often the analysis is repeated.
10. Conclusion	Summary of the key findings and recommendations, and the next steps towards the target state.
11. Appendices (optional)	Detailed data, charts, tables, and supporting documentation (e.g., audit and penetration test results, training records).

14.2. Example: Gap Analysis Report

1—3 Introduction, Methodology, Current state

Purpose — verify compliance with Act No. 264/2025 Coll. and ISO/IEC 27001:2022. Scope — data protection, access control, incident response, cybersecurity awareness. Reference framework — ISO/IEC 27001:2022 and NIS2. Current state — data stored unencrypted, passwords only, no incident response plan, low employee awareness.

4—5 Identified gaps and causes

Gaps — no encryption software, no MFA solution, no incident response plan, insufficient

training. Root causes — underinvestment in encryption technologies, low awareness of MFA benefits, unclear process ownership.

6—8 Measures, timeline, responsibilities

Implement encryption (IT department, 3 months); deploy MFA (security team, 2 months); build and test an incident response plan (incident response team, 4 months); run awareness training (HR with IT, ongoing).

9—11 Monitoring, conclusion, appendices

KPIs — number of incidents and incident response time, phishing test results, audit and penetration test outcomes. Next steps — track the action plan and repeat the analysis annually. Appendices — audit results, test reports, training records.