EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TECHNICAL IMPLEMENTATION GUIDANCE

On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards **technical and methodological requirements of cybersecurity risk-management measures**

JUNE 2025, VERSION 1.0

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, use ENISA-NIS-Directive@enisa.europa.eu.
For media enquiries about this paper, use press@enisa.europa.eu.

AUTHORS

Konstantinos Moulinos, Marianthi Theocharidou, ENISA

ACKNOWLEDGEMENTS

This publication was developed by ENISA, in collaboration with the European Commission and the Network and Information Systems Cooperation Group. ENISA would like to thank for their efforts the Network and Information Systems Cooperation Group, along with the ENISA European Competent Authorities for Trust Services Expert Group and the European Competent Authorities for Secure Electronic Communications. Moreover, ENISA would like to recognise the valuable feedback of the individuals, private organisations, associations and members of the open source software community that contributed to the open consultation.

LEGAL NOTICE

Luxembourg: Publications Office of the European Union, 2025

COPYRIGHT NOTICE

ISBN 978-92-9204-704-7, doi:10.2824/2702548

EXECUTIVE SUMMARY

Under the NIS2 Directive, EU member states set requirements for cybersecurity risk management measures at national level in critical sectors, for example digital infrastructures, energy, transport or health. However, for several subsectors of the digital infrastructures and the ICT service management sectors, these requirements are set at European Union level due to their cross-border nature. For this purpose, the European Commission published the Implementing Regulation (EU) 2024/2690 on 17 October 2024 ([1]), which lays down the technical and methodological requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555. The technical and methodological requirements are set out in Article 2 and in the Annex to this implementing regulation.

This technical guidance supports this implementing regulation by providing:

- guidance, that is, indicative and actionable advice on parameters to consider when implementing a requirement;
- examples of evidence, that is, the types of evidence that a requirement is in place; and
- mappings from security requirements to industry good practices, European and international standards, and national frameworks.

The document, as well as the implementing regulation, refers to the following type of entities:

- domain name system service providers,
- top-level domain name registries,
- cloud computing service providers,
- data centre service providers,
- content delivery network providers,
- managed service providers and managed security service providers,
- providers of online marketplaces, online search engines and social networking services platforms and
- trust service providers.

The document covers the following technical and methodological requirements:

1. policy on the security of network and information systems,
2. risk management policy,
3. incident handling,
4. business continuity and crisis management,
5. supply chain security,
6. security in network and information systems acquisition, development and maintenance,
7. policies and procedures to assess the effectiveness of cybersecurity risk-management measures,
8. basic cyber hygiene practices and security training,
9. cryptography,
10. human resources security,
11. access control,
12. asset management and
13. environmental and physical security.

To develop this technical guidance, ENISA worked closely with the European Commission and the Network and Information Systems Cooperation Group, and ENISA held a public consultation to get input from the private sector. This guidance is a living document because it maps the technical and methodological requirements referred to in Article 2

([1]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2690&qid=1729254262885.

and the Annex to the implementing regulation, to European and international standards and to national cybersecurity management frameworks. Both the standards and the management frameworks are constantly subject to change. Therefore, a review process should be initiated at regular intervals by ENISA in collaboration with the European Commission and the Network and Information Systems Cooperation Group, for instance to add additional mappings industry good practices, international standards and national frameworks.

DISCLAIMER

This document is not legally binding and is only of an advisory character. It is not intended to replace the frameworks, guidance, tools or other mechanisms provided by Member States at national level.

It should be clarified that the Member States retain the freedom to determine their approach to the supervision of the requirements under this implementing regulation. Therefore, this ENISA technical guidance is not able to define whether an entity needs to have all or just some of the 'evidence' listed (although requiring all the 'evidence' listed here would be a very strict approach to supervision). This document also does not determine the appropriateness of such measures or evidence. However, it can help the national competent authorities develop their approach to the supervision of the requirements.

Entities in scope of the regulation should check under whose jurisdiction they fall and they should follow any guidance by national competent authorities (see recital 7 of the implementing regulation).

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

On 18 October 2024, the European Commission published Commission Implementing Regulation 2024/2690 of 17 October 2024, hereafter the **regulation**, pursuant to Articles 21(5), first subparagraph and 23(11), second subparagraph, of Directive (EU) 2022/2555 (hereafter the NIS2 Directive). Article 2 of this regulation specifies that, for the essential and important entities in scope of the regulation (hereafter 'relevant entities'), the technical and methodological requirements of cybersecurity risk-management measures referred to in Article 21(2), points (a) to (j), of the NIS2 Directive are set out in the **Annex to the regulation**.

According to recital 7, the European Union Agency for Cybersecurity (ENISA) can support relevant entities by providing guidance on the implementation of the technical and methodological requirements referred to in the Annex to the regulation. This implementation guidance was developed by ENISA is collaboration with the Network and Information Systems Cooperation Group (NIS CG) and the European Commission. ENISA published an early draft of this guidance as part of a public consultation, to solicit feedback and input from the private sector. ENISA also consulted with various relevant workstreams of the NIS Cooperation group, as well as the ENISA expert group for European Competent Authorities for Trust Services (ECATS) and the ENISA expert group for European Competent Authorities for Secure Electronic Communications (ECASEC).

GOAL

The document provides non-binding guidance for relevant entities to the regulation on the technical and methodological requirements of the cybersecurity risk management measures.

TARGET AUDIENCE

Beyond the relevant entities to the regulation, this guidance may provide indications on the technical and methodological requirements of the cybersecurity risk management measures of the NIS2 Directive, which may be considered useful by other public or private bodies for improving their cybersecurity.

STRUCTURE

The Annex to the regulation consists of 13 titles with a varying number of technical and methodological requirements (see Figure 1). Each technical and methodological requirement is highlighted (blue font and grey background) and is included in this document for readability.

Each requirement is followed by three elements: guidance, examples of evidence and tips ([2]). This part of the document is not legally binding and is only recommendations ([3]).

1. The **guidance** section contains indicative and actionable advice on parameters to consider when implementing a technical and methodological requirement or further explanation of concepts found in the legal text.
2. **Examples of evidence** are indicative types of evidence showing that a technical and methodological requirement is in place.

(2) A few requirements might not have one or more of these elements because their implementation was considered straightforward.
(3) A recommendation is defined as an 'expression, in the content of a document, that conveys a suggested possible choice or course of action deemed to be particularly suitable without necessarily mentioning or excluding others'.
A requirement is defined as an 'expression, in the content of a document, that conveys objectively verifiable criteria to be fulfilled and from which no deviation is permitted if conformance with the document is to be claimed' (ISO/IEC Directives, Part 2 – Principles and rules for the structure and drafting of ISO and IEC documents, 9th edition, 2021).

3. In some technical and methodological requirements, extra general **tips** are also offered for additional consideration by the entity.

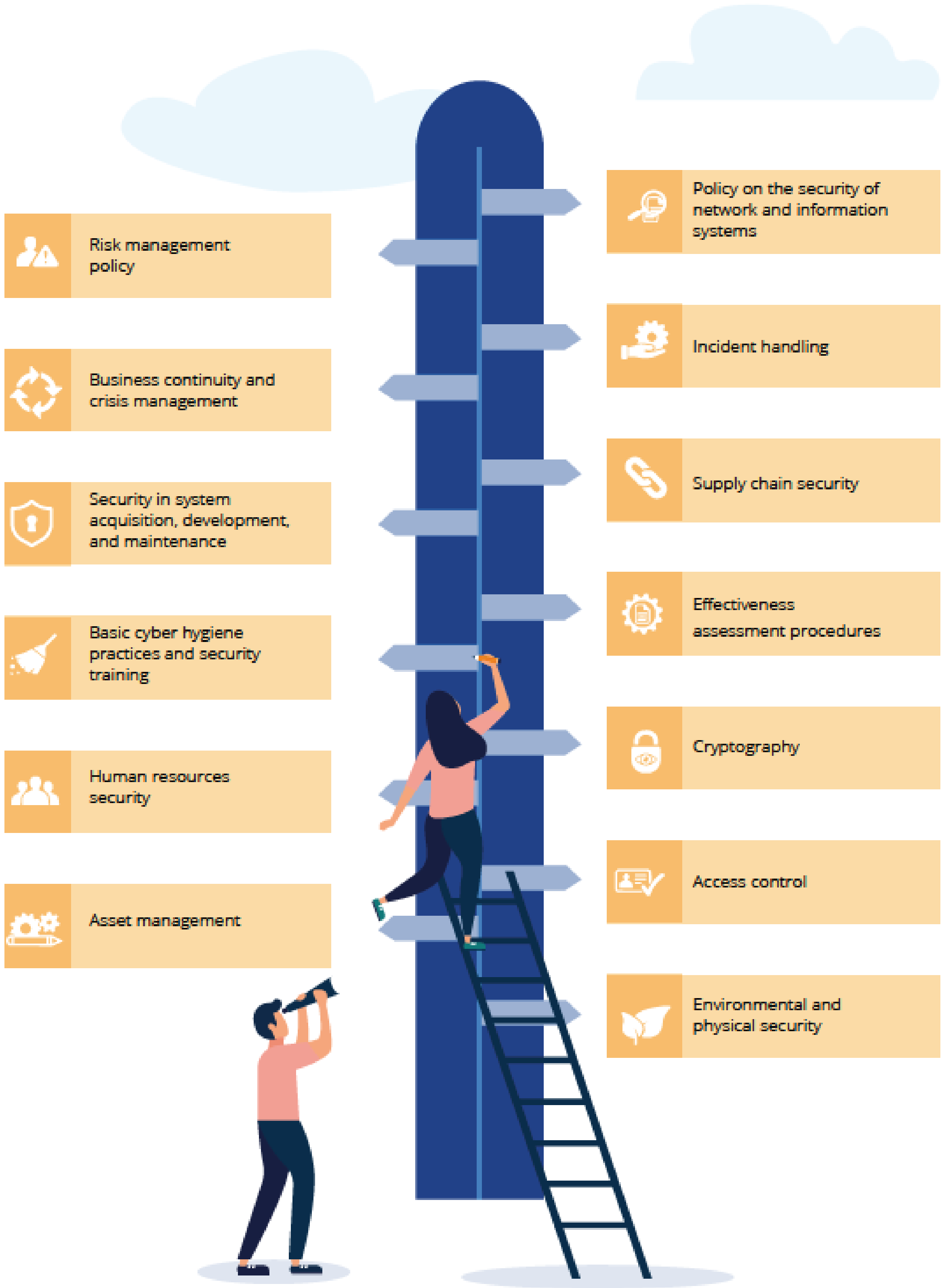

Figure 1: Technical and methodological requirements of the cybersecurity risk-management measures
(Annex to Commission Implementing Regulation 2024/2690)

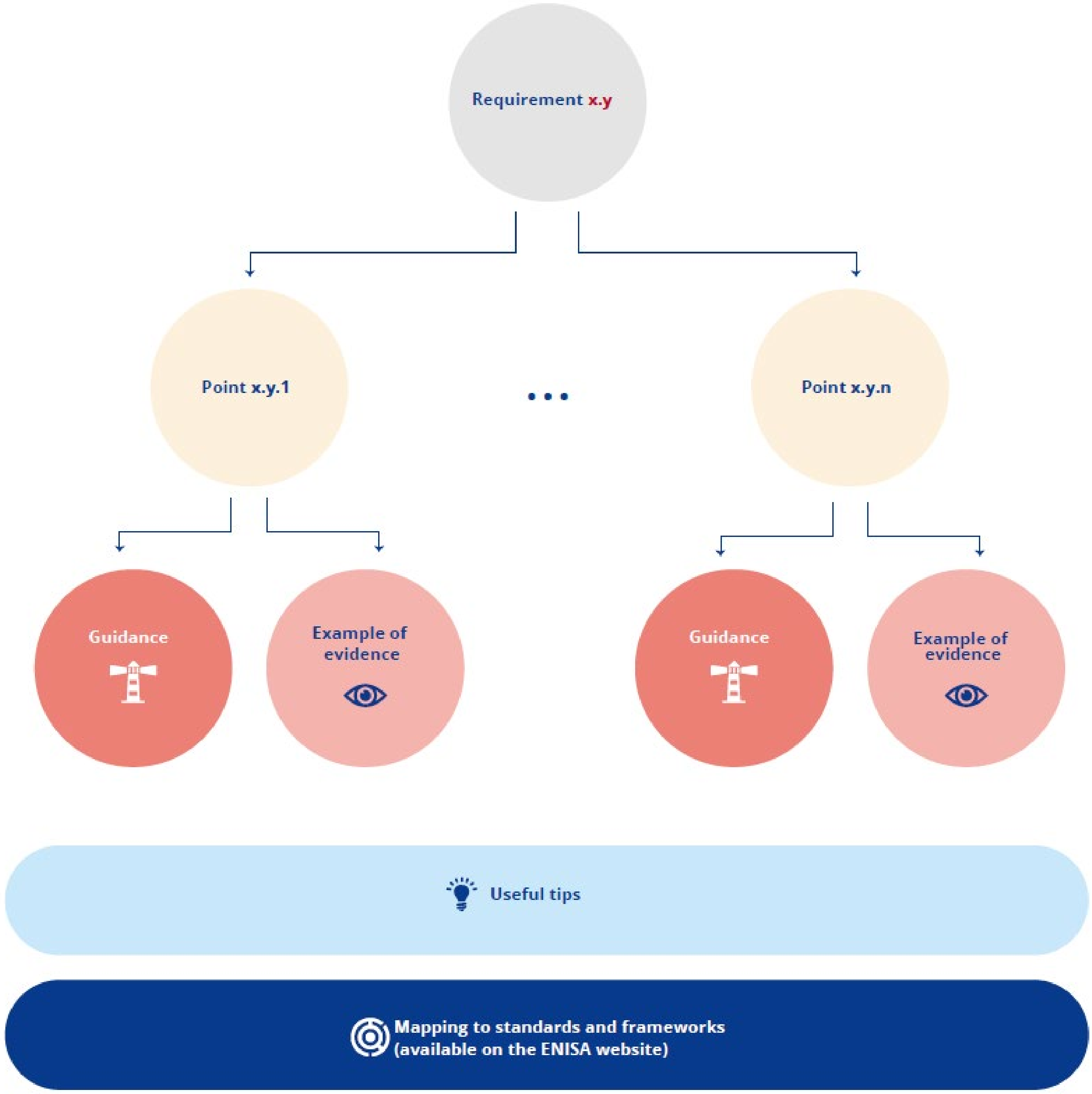

Figure 2: Technical and methodological measures structure

The guidance, examples of evidence and tips are non-exhaustive. Their partial or complete implementation does not assume compliance or conformity with the requirements of the regulation. Relevant entities may choose alternative methods to fulfil a requirement or use different evidence to demonstrate compliance. Moreover, a single piece of evidence may support various requirements; for example, an organisational chart can demonstrate both 'roles and responsibilities' and 'segregation of duties'. Consequently, evidence may appear multiple times within the text.

Finally, each requirement is mapped to (a) requirements of **European and international standards or frameworks** (International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27001:2022, ISO/IEC 27002:2022 ([4]), NIST Cybersecurity Framework 2.0, ETSI EN 319 401 V3.1.1 (2024–06), European Committee for Standardization Technical Specification (CEN/TS) 18026:2024) and (b) to the **NIS2 national frameworks** ([5]). The **mapping to standards and frameworks** is available on the ENISA website in Excel format ([6]). It should be noted that the mapping was done only to horizontal standards and for specific topics. Detailed standards or technical specifications are referenced in footnotes, where available. These standards are included as examples, as they are commonly used. The choice of which standards and good practices to apply should be made by the entity, as they may relate to the context of the entity's activities and characteristics.

To implement the requirements, the relevant entities may build upon their current usage of standards or frameworks, if available. Annex I of this document provides details for each national framework submitted to ENISA during the consultation phases, while some terms are explained in Annex II. The document does not aim to establish a new standard or to duplicate existing ones (e.g. ISO, IEC and CEN). The guidance is written in a technology-neutral and standards-neutral way.

The mapping should not be interpreted as a measure of equivalency among different standards or frameworks. It simply refers to relevant requirements in these standards or frameworks without assessing whether these fully cover the requirements of the regulation. Cybersecurity standards or frameworks often address the same cybersecurity concerns but use different language, structures or levels of specificity or detail. Understanding these relationships may help relevant entities use and integrate multiple standards or frameworks efficiently, to maintain compliance, reduce duplication and streamline audits.

Relevant entities subject to the regulation can use national frameworks, guidance, standards or other mechanisms equivalent to the requirements of the regulation to demonstrate their compliance to national competent authorities. Depending on the national framework, compliance with the requirements set out by the regulation could be demonstrated by means of assessment or certification by relevant accredited conformity assessment bodies or by independent auditors authorised by the national competent authorities or certification bodies authorised by the national competent authorities, against the national frameworks, guidelines, standards or other mechanisms equivalent to technical and methodological requirements for cybersecurity risk-management measures. To keep the current guidance up to date, Member States can inform ENISA of those equivalent national frameworks, guidance, standards or other mechanisms, if available.

TOPIC-SPECIFIC POLICIES

As described in preamble 9 of the regulation, the **policy on the security of network and information systems** ([7]) (Annex to the regulation, point 1.1) should be the highest-level document setting out the relevant entities' overall approach to the security of their network and information systems and should be approved by the management bodies of the entities.

([4]) The information security controls listed in Table A.1 of Annex A to this standard are directly derived from and aligned with those listed in ISO/IEC 27002:2022. Clauses 5 to 8 are to be used in context with clause 6.1.3 (information security risk treatment) of ISO/IEC 27001:2022.
([5]) The mapping is based on the information that the representatives of the Member States in the NIS Cooperation Group work stream on security measures have provided to ENISA.
([6]) ENISA Technical implementation guidance mapping table (Excel file), https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
([7]) Article 21(2), point (a) of the NIS2 Directive.

In addition to this overarching corporate policy, the following topic-specific, documented policies ([8]) are required.

1. **Risk management policy** (Annex to the regulation, point 2).
2. **Incident handling policy** (Annex to the regulation, point 3.1.1).
3. **Supply chain security policy** (Annex to the regulation, point 5.1.1).
4. **Security testing policy** (Annex to the regulation, point 6.5.1).
5. **Policy to assess the effectiveness of cybersecurity risk management measures** (Annex to the regulation, point 7.1.1).
6. **Policy related to cryptography** (Annex to the regulation, point 9.1).
7. **Access control policy** (Annex to the regulation, point 11.1.1).
8. **Policies for the management of privileged accounts and system administration accounts** (Annex to the regulation, point 11.3)
9. **Handling of information and assets policy** (Annex to the regulation, point 12.2.1).
10. **Removable media policy** (Annex to the regulation, point 12.3.1).

Documenting the aforementioned topic-specific policies is mandatory. However, the relevant entity should use its discretion to determine the format of documentation, whether it be through separate documents, updates to existing policies or a single comprehensive document.

([8]) According to ISO/IEC 27002:2022, topic-specific policy includes 'intentions and direction on a specific subject or topic, as formally expressed by the appropriate level of management'.

POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

1. POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

1.1 POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

1.1.1. For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the policy on the security of network and information systems shall:

(a) set out the relevant entities' approach to managing the security of their network and information systems;

(b) be appropriate to and complementary with the relevant entities' business strategy and objectives;

(c) set out network and information security objectives;

(d) include a commitment to continual improvement of the security of network and information systems;

(e) include a commitment to provide the appropriate resources needed for its implementation, including the necessary staff, financial resources, processes, tools and technologies;

(f) be communicated to and acknowledged by relevant employees and relevant interested external parties;

(g) lay down roles and responsibilities pursuant to point 1.2;

(h) list the documentation to be kept and the duration of retention of the documentation;

(i) list the topic-specific policies;

(j) lay down indicators and measures to monitor its implementation and the current status of relevant entities' maturity level of network and information security;

(k) indicate the date of the formal approval by the management bodies of the relevant entities (the 'management bodies').

GUIDANCE

- Set a policy on the security of network and information systems, covering all systems, assets and procedures that fall within the scope of the policy.
- Make sure that relevant personnel and relevant interested external parties, acknowledge the policy on the security of network and information systems, typically through a signed document or digital acknowledgement, where applicable.
  - Depending on the context, external parties may mean suppliers, service providers, shareholders, authorities, visitors, external interest groups or forums.
  - The acknowledgement may be included in other contracts, such as employment contracts or service provision contracts.
  - The policy should be communicated to relevant personnel and interested external parties in a form that is relevant, accessible and understandable to the intended reader.
  - Relevant personnel and relevant interested external parties may not be made aware of the full text of the policy. Depending on their role, an extract or a summary containing only relevant information should be communicated and acknowledged. If the policy is distributed outside the entity, care should be taken not to disclose confidential information.
  - For contractual requirements of direct suppliers and service providers, point 5.1.4 of the Annex to the regulation.

- Make sure that personnel are aware of their responsibilities for the security of network and information systems.
- Make sure that the policy on the security of network and information systems is approved by the management bodies.
- Make sure that the topic-specific policies are approved by an appropriate level of management.
- Make sure that the policy includes detailed guidance on the procedures for managing policy exceptions.

EXAMPLES OF EVIDENCE

- Documented policy on the security of network and information systems which contains the elements required by points 1.1.1 (a) to 1.1.1 (k) of the Annex to the regulation.
- The date of the formal approval by the management bodies of the relevant entities, indicated in the policy on the security of network and information systems.
- Where applicable, acknowledgement forms or employment contracts, signed by personnel, which confirm they have read and understood the security policies.
- Where applicable, acknowledgement forms, service provision contracts or other contracts, signed by relevant interested external parties, which confirm they have read and understood the security policies.
- Evidence that the management bodies understand their role, responsibilities and authorities regarding network and information security. This can include but is not limited to:
    - allocation of resources for policy implementation;
    - requests (e.g. announcements, emails and documents) to personnel to apply network and information security in accordance with the established policies and procedures; and
    - any initiatives that indicate that management bodies promote improvement in the area of network and information security.

1.1.2. The network and information system security policy shall be reviewed and, where appropriate, updated by management bodies at least annually and when significant incidents or significant changes to operations or risks occur. The result of the reviews shall be documented.

GUIDANCE

- Review the policy on the security of network and information systems at least annually, taking into account (indicative, non-exhaustive list):
    - updates to the risk assessment results and the risk treatment plan (Annex to the regulation, point 2.1.4);
    - relevant changes in legislation (laws, regulations and other measures imposed by national competent authorities);
    - recommendations provided by relevant authorities;
    - relevant changes in industry good practices;
    - feedback from interested parties;
    - findings of compliance monitoring (section 2.2) and of independent reviews (Annex to the regulation, point 2.3), including policy violations or policy exceptions;
    - incidents, even those affecting similar entities in the sector.

- Update the policy on the security of network and information systems and topic-specific policies, in line with new findings that could affect the entity's approach to managing information security, including ([9]):
  - updates to the risk assessment results and the risk treatment plan (Annex to the regulation, point 2.1.4);
  - changes to the network and information systems;
  - changes to the environment of operation;
  - problems identified during the implementation of the policy;
  - findings of compliance monitoring (Annex to the regulation, point 2.2.1) and of independent reviews (Annex to the regulation, point 2.3), including policy violations or policy exceptions;
  - the status of preventive and corrective actions;
  - trends related to threats and vulnerabilities; and
  - known reported security incidents.
- All updates to the policy should be based on the covered entity's unique security risks identified through its risk assessment.
- Obtain approval for the revised policy and the policy exceptions by the management bodies.

EXAMPLES OF EVIDENCE

- Review comments or change logs for the policy on the security of network and information systems and topic-specific policies.
- Documentation of the review process of the requirements listed in point 1.1.1 of the Annex to the regulation.
- Up-to-date policy on the security of network and information systems and topic-specific policies.
- Evidence that any updates to the policy on the security of network and information systems and any policy exceptions, are approved by management bodies and a record is kept.
- Evidence that any updates to the topic-specific policies are approved by an appropriate level of management and a record is kept.
- Records of the management review.

TIPS

GUIDANCE

- Analyse the policy on the security of network and information systems for compliance with:
  - legislative, regulatory and contractual requirements;
  - awareness and training requirements (Annex to the regulation, points 8.1 and 8.2); and
  - business continuity requirements (Annex to the regulation, point 4.1).
- Define procedures to facilitate the implementation of the policy on the security of network and information systems and associated measures.
- Examine documentation of post-incident reviews for significant incidents ([10]) that include participation and input from management bodies.
- Ensure that the policy is:

([9]) The occurrence of the indicative events provided does not automatically require a covered entity to update its policy. Instead, the occurrence of such events should be considered through the risk-assessment process, allowing the entity to determine whether new policy updates are necessary to address its unique security risks identified by the risk assessment.
([10]) In accordance with Articles 3 and 5-14 of the regulation.

- protected in terms of confidentiality (on a need-to-know basis), integrity, availability and authenticity;
- managed properly so the information is complete, correct, understandable, easily identifiable and retrievable.

EXAMPLES OF EVIDENCE

- Documented policy on the security of network and information systems, including networks and services in scope, assets supporting them and the security objectives, including applicable laws and regulations, accessible to personnel.
- Documented topic-specific policies, including applicable laws and regulations, accessible to relevant personnel.
- Evidence of cybersecurity training of management, for instance:
  - training records;
  - workshop and seminar attendance; and
  - continuous learning materials.
- Internal communication logs, ad hoc reports or communication policy or records showing regular briefings or updates provided to management bodies regarding cybersecurity matters or during significant incidents.

1.2 ROLES, RESPONSIBILITIES AND AUTHORITIES

1.2.1. As part of their policy on the security of network and information systems referred to in point 1.1, the relevant entities shall lay down responsibilities and authorities for network and information system security and assign them to roles, allocate them according to the relevant entities' needs and communicate them to the management bodies.

GUIDANCE

- Write job descriptions in a way that clearly outlines rights and responsibilities.
- Assign security roles and responsibilities to personnel and include these roles in the organisational chart.
- Describe roles and assign corresponding responsibilities (e.g. chief information security officer), based on the guidance of international frameworks and standards, including the European cybersecurity skills framework (ECSF) ([11]).
- Ensure that the roles allocated are suitable for the size and business needs of the entity.
- Formally appoint competent personnel in security roles. Ensure that these assigned persons are competent on the basis of appropriate education, training or experience.

EXAMPLES OF EVIDENCE

- Job descriptions.
- List of security roles, who occupies them and contact information.
- Formal appointment of the key security roles and responsibilities, for example, listed in the company organigram or management decision, etc.
- List of appointments and description of responsibilities and tasks for security roles.
- Evidence of competence of the assigned persons.

([11]) https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf.

1.2.2. The relevant entities shall require all personnel and third parties to apply network and information system security in accordance with the established network and information security policy, topic-specific policies and procedures of the relevant entities.

GUIDANCE

- Make personnel aware of the security roles in the entity and when each role should be contacted.
- Make personnel aware of their network and information system security obligations, according to their role. For the disciplinary process, see point 10.4 in the Annex to the regulation.
- Make relevant interested external parties aware of their network and information system security obligations.
    - For contractual requirements of direct suppliers and service providers, see point 5.1.4 in the Annex to the regulation.
    - Consider third parties, which means external entities or organisations not directly involved in the operations of the entity in scope but that may still affect its network and information security. For examples of relevant interested external parties, consider the guidance in section 1.1.
- The requirement that all personnel and third parties apply network and information system security should be communicated in a form that is relevant, accessible and understandable to the intended reader.
    - The network and information security policy, topic-specific policies and procedures of the relevant entities do not necessarily need to be communicated in their entirety.

EXAMPLES OF EVIDENCE

- Awareness/dissemination material for personnel, explaining security roles and when/how they should be contacted.
- Service level agreements (SLAs), contracting contracts, data-processing agreements or other types of contracts or agreements with third parties.
- Acknowledgement from third parties in various forms (letters, emails, portals or other online options) confirming that they have received and understand their obligations related to network and information system security, where such requirements are not covered by contractual arrangements.

1.2.3. At least one person shall report directly to the management bodies on matters of network and information system security.

GUIDANCE

- Appoint a person (e.g. chief information security officer or information security manager) responsible for overseeing network and information security matters.
- Make sure that this role is recognized and duly authorized by management bodies.

EXAMPLES OF EVIDENCE

- Up-to-date documentation of the structure of security role assignments and responsibilities.
- Minutes from meetings with the management.
- Evidence of business decisions made (e.g. investments in cybersecurity).

1.2.4. Depending on the size of the relevant entities, network and information system security shall be covered by dedicated roles or duties carried out in addition to existing roles.

GUIDANCE

- It is often practical to have dedicated information security roles (e.g. a chief information security officer or security analysts) who focus solely on protecting the entity's data and systems.
- In entities with limited resources, information security responsibilities may be distributed among existing roles. For instance, information technology (IT) staff might take on security duties alongside their regular tasks. However, the persons assigned should have relevant experience and training to perform the roles and to exercise their responsibilities.

EXAMPLES OF EVIDENCE

- Verify the presence of dedicated security roles in larger entities.
- Check if security responsibilities are assigned to existing roles in smaller entities.

1.2.5. Conflicting duties and conflicting areas of responsibility shall be segregated, where applicable.

GUIDANCE

- Consider segregating conflicting duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of the entity's asset. As a minimum, consider that the reviewer (auditor) must be different from the personnel or the line of authority of the area under review.
- The results of the risk assessment or the business impact analysis (BIA) could be used to identify potential conflicting duties and areas of responsibility.

EXAMPLES OF EVIDENCE

- Up-to-date documentation of the structure of security role assignments and responsibilities.

1.2.6. Roles, responsibilities and authorities shall be reviewed and, where appropriate, updated by management bodies at planned intervals and when significant incidents or significant changes to operations or risks occur.

GUIDANCE

- Regularly review and revise the structure of security roles and responsibilities, based on (indicative, non-exhaustive list):
    - significant incidents, if any;
    - changes to the environment of operation, including changes to the network and information systems;
    - organisational changes.
- Where appropriate, updates should be approved by management bodies.

EXAMPLES OF EVIDENCE

- Up-to-date documentation of the structure of security role assignments and responsibilities, including version history.
- Documentation of the review process, taking into account changes and past incidents.

TIPS

GUIDANCE

- Make sure that the roles responsible for security roles are contactable in case of incidents.
- Make sure that each role has its deputy or that measures ensuring continuity in the event of the role representative's absence are in place, where possible.
- Establish a clear reporting line from the designated security officer to senior management.
- Ensure that security reporting is integrated into the entity's overall risk management framework.

EXAMPLES OF EVIDENCE

- Documented incident response procedures (Annex to the regulation, point 3.5.1) including clear procedures for contacting security roles during an incident.
- Logs and records of past incidents to check if the security roles were contacted promptly and effectively.
- Crisis management process and incident response records to check the involvement of the management.
- Up-to-date organisational chart to check if it clearly shows the reporting structure, including the designated security officer and their direct line to senior management. The organisational chart should be dated and the person making the update should be noted.

RISK MANAGEMENT POLICY

2. RISK MANAGEMENT POLICY

2.1 RISK MANAGEMENT FRAMEWORK

2.1.1. For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the relevant entities shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems. The relevant entities shall perform and document risk assessments and, based on the results, establish, implement and monitor a risk treatment plan. Risk assessment results and residual risks ([12]) shall be accepted by management bodies or, where applicable, by persons who are accountable and have the authority to manage risks, provided that the relevant entities ensure adequate reporting to the management bodies.

GUIDANCE

- The entity can use its current risk management framework or adopt a new one ([13]). A risk management framework is the structured approach used by an entity to identify, assess, manage and mitigate its cybersecurity risks.
- Create a risk treatment plan that associates the identified risks with assets and the measures mitigating the associated risks and takes into account, at least, elements (g) to (h) in point 2.1.2 of the Annex to the regulation. The plan should at least include:
    - a description of the identified risk and how it can negatively affect security objectives;
    - a risk treatment option (for example risk avoidance, risk mitigation, risk transfer or sharing or risk acceptance);
    - the assets associated with the risk;
    - the measures which mitigate the risk;
    - a procedure for assessing the effectiveness of implementation of the measure(s);
    - implementation timelines; and
    - responsible roles.
- Consider residual risks from third parties, for example, data breaches, unaddressed vulnerabilities, regulatory non-compliance from the from the third-party side and over-reliance on a single third party.
- Ensure residual risks are accepted by management bodies or, where applicable, persons who are accountable and have the authority to manage risks, in line with the acceptable residual risk levels of the entity.
- Make sure that management bodies or, where applicable, persons who are accountable and have the authority to manage risks approve the risk-assessment results and risk-treatment plan.

EXAMPLES OF EVIDENCE

- Documented risk management framework.
- Documented results from previous risk assessments.
- Documented risk treatment plan.

([12]) The remaining risk after management has implemented a risk response. Source: ISACA Glossary, https://www.isaca.org/resources/glossary.
([13]) For example, ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks. A collection of frameworks and methodologies that provide high-level guidelines for risk-management processes that can be applied in all types of organisations is available at https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks.

- Record of approval of risk assessment results by management bodies or by persons who are accountable and have the authority to manage risks.
- Record of approval of residual risks by management bodies or, where applicable, by persons who are accountable and have the authority to manage risks.

2.1.2. For the purpose of point 2.1.1, the relevant entities shall establish procedures for identification, analysis, assessment and treatment of risks ('cybersecurity risk management process'). The cybersecurity risk management process shall be an integral part of the relevant entities' overall risk management process, where applicable. As part of the cybersecurity risk management process, the relevant entities shall:
(a) follow a risk management methodology;
(b) establish the risk tolerance level in accordance with the risk appetite of the relevant entities;
(c) establish and maintain relevant risk criteria;
(d) in line with an all-hazards approach, identify and document the risks posed to the security of network and information systems, in particular in relation to third parties and risks that could lead to disruptions in the availability, integrity, authenticity and confidentiality of the network and information systems, including the identification of single point of failures;
(e) analyse the risks posed to the security of network and information systems, including threat, likelihood, impact and risk level, taking into account cyber threat intelligence and vulnerabilities;
(f) evaluate the identified risks based on the risk criteria;
(g) identify and prioritise appropriate risk treatment options and measures;
(h) continuously monitor the implementation of the risk treatment measures;
(i) identify who is responsible for implementing the risk treatment measures and when they should be implemented;
(j) document the chosen risk treatment measures in a risk treatment plan and the reasons justifying the acceptance of residual risks in a comprehensible manner.

GUIDANCE

- Select a risk management methodology ([14]).
- Establish the entity's risk appetite, that is the amount of risk that the entity is strategically willing to accept to achieve its objectives. Criteria may include (indicative, non-exhaustive list):
  - business strategic objectives;
  - stakeholder expectations;
  - regulatory requirements; and
  - organizational culture.
- Define the risk tolerance level, which refers to the level of risk that an entity is willing to accept in pursuit of its long-term objectives. Examples may include (indicative, non-exhaustive list):
  - acceptable downtime for systems for which criticality is high (e.g. up to two hours of downtime per month);
  - tolerance for data loss (e.g. loss of data with low criticality within a 24-hour window);
  - maximum financial loss that can be absorbed without jeopardizing operations (e.g. up to EUR 100,000 in recovery costs);

([14]) There are many risk-management standards, frameworks and methodologies. A non-exhaustive list of them can be found in the ENISA publication Compendium of risk-managements frameworks with potential interoperability, https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks.

- willingness to invest a certain percentage of revenue in measures (e.g. 5% of annual revenue);
- adherence to regulatory obligations with specific penalties or fines influencing risk acceptance;
- acceptable level of customer dissatisfaction or negative media exposure from a data breach (e.g. tolerating one major incident every few years);
- acceptance of certain vulnerabilities based on risk mitigation measures in place (e.g. outdated software provided that it is monitored and patched regularly);
- time frame for responding to and recovering from incidents (e.g. a maximum of 48 hours for containment); and
- acceptance of minor incidents as part of normal operations while prioritizing major threats.

- Define risk acceptance criteria, which may include (indicative, non-exhaustive list) ([15]):
  - accepting risks categorized as low severity, such as minor data leaks that don't expose sensitive information;
  - accepting risks assessed as having a low likelihood of occurrence (e.g. certain rare types of cyberattacks);
  - accepting risks if the cost of mitigation exceeds the potential impact (e.g. not upgrading legacy systems if the upgrade cost is significantly higher than potential losses);
  - accepting specific compliance risks if there is a plan in place to address them within a defined timeframe (e.g. temporarily accepting minor non-compliance with a commitment to remediate within six months);
  - allowing certain risks in low-criticality systems or departments that do not affect core business operations (e.g. accepting a risk in a test environment);
  - accepting certain vulnerabilities for a defined period while planning for remediation (e.g. accepting the risk of outdated software for three months until a full upgrade can be completed);
  - accepting risks where the expected incident impact falls below a predetermined financial threshold (e.g. losses under EUR 50,000 accepted without further action);
  - accepting risks after informing stakeholders and receiving their agreement, particularly if they understand the trade-offs involved; and
  - accepting residual risks where existing measures reduce the likelihood or impact to an acceptable level (e.g. using encryption for sensitive data but accepting risks of loss due to user error).
- Define risk criteria, that is, how the entity evaluates the significance of the risks that it identifies and makes decisions concerning risks. Risk criteria may include (indicative, non-exhaustive list):
  - alignment with risk appetite: accepting risks that align with the organization's overall risk appetite, such as delays in internal reporting processes that do not impact customer service or compliance;
  - regulatory and legal exposure: prioritizing risks based on potential legal or regulatory consequences, such as treating violations of the General Data Protection Regulation (GDPR) involving customer data as high-risk due to potential fines and reputational damage;
  - reputational impact: escalating risks that could significantly harm the organization's public image, such as incidents likely to attract media attention;
  - risk velocity: giving higher priority to risks with high velocity, such as zero-day exploits that can be weaponised before patches are available;

([15]) More information on risk criteria can be found in ISO/IEC 27005:2022, paragraph 6.4. It is important to understand that risk appetite, defined as the amount of risk an entity is willing to pursue or accept, can vary considerably from entity to entity. For instance, factors affecting an entity's risk appetite include size, complexity and sector.

   - recovery complexity: treating risks as critical if they involve complex or time-consuming recovery, such as cyber-attacks on legacy systems with limited vendor support;
   - emerging technology risks: Considering risks involving emerging technologies as higher priority, such as AI systems producing unexplainable or non-compliant decisions due to lack of transparency;
   - stakeholder sensitivity: re-evaluating risks that concern key stakeholders, such as risks flagged by the board, regulators or major customers, even if the assessed technical risk is low.
- Criteria for performing cybersecurity risk assessments refer to consequences, likelihood or level of risk. These may refer to (indicative, non-exhaustive list):
   - the importance of assets;
   - the severity of threats;
   - the vulnerability of network and information systems ([16]);
   - impact analysis;
   - existing measures; and
   - stakeholders concerns or requirements.
- Make a list of the main risks for the security of network and information systems, taking into account the main threats to the assets in scope.
- Make sure that each risk is associated with at least one:
   - of the risk treatment options or a combination of them, in line with the results of the risk assessment and in accordance with the entity's policy on the security of network and information systems (recital 11 of the regulation); and
   - specific risk treatment measure.
- Develop risk-treatment plans to address the elements in points (i) and (j) in point 2.1.2 of the Annex to the regulation.
- Assign responsibilities to appropriate individuals or teams for executing these risk treatment plans.

EXAMPLES OF EVIDENCE

- Documented cybersecurity risk-management process that takes into account elements referred to in point 2.1.2 of the Annex to the regulation.
- Documented risk-management methodology and/or tools that take into account at least elements (a) to (f) in point 2.1.2 of the Annex to the regulation.
- List of the main risks described at a high level, including underlying threat(s) and unaddressed vulnerabilities and their potential impact on the security of networks and services.
- Make sure that the entity follows an all-hazards approach (check that the risk-assessment approach addresses a wide range of potential threats and risks, not just the cyber ones, but natural or man-made, accidental or intentional threats and risks).
- Evidence that residual risks resulting from dependencies on third parties are listed and mitigated.

([16]) Vulnerabilities of network and information systems may also arise from human, organizational, and procedural weaknesses.

2.1.3. When identifying and prioritising appropriate risk treatment options and measures, the relevant entities shall take into account the risk assessment results, the results of the procedure to assess the effectiveness of cybersecurity risk-management measures, the cost of implementation in relation to the expected benefit, the asset classification referred to in point 12.1 and the business impact analysis referred to in point 4.1.3.

GUIDANCE

- Make sure that personnel take into account the elements referred to in point 2.1.3 of the Annex to the regulation.

EXAMPLES OF EVIDENCE

- Guidance for personnel on assessing risks that takes into account the elements referred to in point 2.1.3 of the Annex to the regulation.

2.1.4. The relevant entities shall review and, where appropriate, update the risk assessment results and the risk treatment plan at planned intervals and at least annually and when significant changes to operations or risks or significant incidents occur.

GUIDANCE

- Review risk assessment results and risk treatment at least annually taking into account:
  - results of audits and previous reviews,
  - status of implementation of the measures described in the risk treatment plan (see the policy on the assessment of the effectiveness of measures in line with the Annex to Regulation, point 7.1.1);
  - changes to the information systems;
  - changes to the environment of operation;
  - post-incident review findings (section 3.6); and
  - trends and changes related to threats and vulnerabilities, as they may affect risks.

EXAMPLES OF EVIDENCE

- Documentation of the review process.
- Review comments or change logs for the risk assessment and risk treatment plan.

TIPS

GUIDANCE

- Ensure that key personnel use the risk management methodology and tools.
- Overall, the entity has four risk treatment options associated with each risk. Each option should be accompanied by specific risk treatment measures (indicative, non-exhaustive list of examples):
  - Risk avoidance: as a measure to treat this risk, the entity might choose to eliminate activities or conditions that expose the entity to this risk, for example, discontinuing the use of a vulnerable software application.
  - Risk mitigation: as a measure to treat this risk, the entity might choose to implement measures to reduce the likelihood or impact of such a risk. This can include installing firewalls, using encryption and conducting regular security training for employees.

- Risk transfer or sharing: as a measure to treat this risk, the entity might choose to shift parts of the risk impact to another party, typically through insurance or outsourcing certain functions to third-party providers. However, it is important to note that such arrangements do not eliminate the entity's overall accountability or legal obligations regarding the risk. For instance, purchasing cyber insurance may cover potential data breach costs, but the entity remains responsible for implementing appropriate security measures and complying with data protection regulations.
- Risk acceptance: as a measure to treat this risk, the entity might choose to acknowledge the risk and decide to accept it without taking any specific action, often because the cost of mitigation is higher than the potential impact. This approach is usually accompanied by a contingency plan to manage the risk if it materialises. The approach should be clearly documented, supported by a realistic estimation of potential costs and including financial provisions to address the impact should the risk materialise.

- Make sure that the risk from vulnerabilities assigned to the highest classification (e.g. 'critical' in the common vulnerability scoring system (CVSS)) or equivalent is not accepted, if possible (section 6.10).
- Concerning the risk treatment plans, the entity might additionally take into account:
  - findings of the review;
  - implementation steps; and
  - resources needed.
- Manage any exceptions in the risk treatment plans' implementation.

EXAMPLES OF EVIDENCE

- Documented action plans developed in response to review findings.
- Key personnel knowing the main risks (e.g. evidence from emails, interviews and awareness-raising sessions).
- Documented risk treatment plan implementation exceptions.
- Risk register.

2.2 COMPLIANCE MONITORING

2.2.1. The relevant entities shall regularly review the compliance with their policies on network and information system security, topic-specific policies, rules and standards. The management bodies shall be informed of the status of network and information security on the basis of the compliance reviews by means of regular reporting.

GUIDANCE

- Develop a standardized report format for reporting to management bodies. Consider the following elements (indicative, non-exhaustive list):
  - key metrics,
  - compliance status, including policy exceptions,
  - identified risks and
  - recommended actions.
- Reports are generated and presented to management bodies at least annually.

EXAMPLES OF EVIDENCE

- Recent compliance review reports.

- Logs of policy exceptions. Examples of such exceptions include, among others, the situations mentioned in the second paragraph of Article 2(2) and those under recital 5 of the regulation. Other examples include (indicative, non-exhaustive list):
  - software updates: if a system relies on an older version of software that is incompatible with the latest update, an exception might be granted to delay the update until a compatible solution is found;
  - access control: if a particular user or system cannot support an authentication mechanism (e.g. multi-factor authentication (MFA)) due to technical limitations, an exception might be granted while alternative measures are implemented; and
  - encryption: if a legacy system does not support encryption, an exception might be granted until the system is replaced.
- Records of the exception request and approval, along with details of the compensatory controls implemented.

2.2.2. The relevant entities shall put in place an effective compliance reporting system which shall be appropriate to their structures, operating environments and threat landscapes. The compliance reporting system shall be capable to provide to the management bodies an informed view of the current state of the relevant entities' management of risks.

GUIDANCE

- Set up procedures for compliance monitoring, including (indicative, non-exhaustive list):
  - objectives and a high-level approach to compliance monitoring;
  - relevant security policies that are subject to compliance monitoring;
  - the frequency of compliance reviews;
  - who should carry out compliance reviews (internal or external); and
  - templates for compliance review reports.
- Analyse and evaluate the results of the compliance review.

EXAMPLES OF EVIDENCE

- Documented procedures for monitoring compliance.
- Documented analysis and evaluation of the results, including the current state of the entity's risk management.
- Detailed compliance monitoring plans, including long-term, high-level objectives and planning.

2.2.3. The relevant entities shall perform the compliance monitoring at planned intervals and when significant incidents or significant changes to operations or risks occur.

GUIDANCE

- Compliance monitoring should take place at least annually, taking into account:
  - significant incidents, if any;
  - changes to the environment of operation;
  - changes to the threat landscape and cybersecurity legal and regulatory requirements;
  - changes to standards; and
  - changes to the policy on the security of network and information systems and/or topic-specific policies.

EXAMPLES OF EVIDENCE

- Any corrective actions resulting from the assessments and tests, including changes to the measures made by the entity once the effectiveness of the measures has been assessed in line with the Annex to the regulation, point 7.1.1.
- Evidence that reports of lessons learned or root cause analysis of past incidents, if any, were taken into account.

2.3 INDEPENDENT REVIEW OF INFORMATION AND NETWORK SECURITY

2.3.1. The relevant entities shall review independently their approach to managing network and information system security and its implementation including people, processes and technologies.

GUIDANCE

- Make sure that the independent review is conducted by a person or persons with the appropriate competences (indicative, non-exhaustive list):
  - cybersecurity technical knowledge, for example cybersecurity frameworks (ISO/IEC 27001, National Institute of Standards and Technology (NIST) cybersecurity framework, etc.),
  - industry knowledge,
  - risk assessment skills,
  - compliance and regulatory knowledge, for example the NIS2 Directive, the GDPR and the Digital Operational Resilience Act,
  - good understanding of good practices in auditing and
  - good understanding of when technical certification and conformance are required and must be documented in the conformance and compliance report, to ensure that global standards are implemented correctly.

EXAMPLES OF EVIDENCE

- Documented results of the review or audit.
- Evidence of the competences of the independent reviewers, for example professional experience and academic qualifications, certifications such as certified information systems auditor, certified information systems security professional, certified information security manager, etc.

2.3.2. The relevant entities shall develop and maintain processes to conduct independent reviews which shall be carried out by individuals with appropriate audit competence. Where the independent review is conducted by staff members of the relevant entity, the persons conducting the reviews shall not be in the line of authority of the personnel of the area under review. If the size of the relevant entities does not allow such separation of line of authority, the relevant entities shall put in place alternative measures to guarantee the impartiality of the reviews.

GUIDANCE

- Set up a process for independent review of information and network security, including (indicative and non-exhaustive list):
  - scope and purpose of the independent reviews (e.g. compliance, risk assessment, policy adherence);
  - methodology of the reviews (e.g. standardised checklist, standard based, ad hoc, how it addresses processes that will be tested in real time for conformance (e.g. cloud service) or those that will be periodically evaluated);

  - review committee's role;
  - frequency of the independent reviews;
  - who should carry out independent reviews (internal or external); and
  - templates for independent review reports.
- Maintain independence in line with point 2.3.2 of the Annex to the regulation;
- Where appropriate, consider alternative measures to the separation of line of authority (indicative and non-exhaustive list):
  - review personnel rotation;
  - set up a review committee with members from different departments;
  - external third-party review service provider.

EXAMPLES OF EVIDENCE

- Documented process for independent review of information and network security.
- Conflict of interest declarations.
- Contracts with external third-party review service providers.
- Detailed independent review plans.

2.3.3. The results of the independent reviews, including the results from the compliance monitoring pursuant to point 2.2. and the monitoring and measurement pursuant to point 7, shall be reported to the management bodies. Corrective actions shall be taken or residual risk accepted according to the relevant entities' risk acceptance criteria.

GUIDANCE

- Analyse and evaluate the results of the independent review.
- Report results to management bodies.
- Use a standardized report format for reporting to the management bodies. Consider the following elements (indicative, non-exhaustive list):
  - executive summary, including the scope and key findings,
  - methodology,
  - detailed findings, including gaps identified and non-compliance issues,
  - recommendations and
  - conclusions.
- Reports are generated and presented to management bodies at least annually.
- Take corrective actions or justify, accept and document residual risks.
- The outcomes of independent reviews should be systematically reflected in the risk assessment results and risk treatment plans (Annex to the regulation, point 2.1). Specifically, when a risk is identified or reassessed through an independent review, the corresponding risk assessment should be updated accordingly. This ensures that the risk profile remains accurate and that any emerging or evolving risks are adequately captured and addressed in the overall risk management framework.

EXAMPLES OF EVIDENCE

- Documented analysis and evaluation of the results, including any residual risks.
- Minutes from past reviews.

- Any corrective actions resulting from the assessments and tests, including changes to the measures made by the entity once the effectiveness of the measures has been assessed in line with the Annex to the regulation, point 7.1.1.
- Documentation of any corrective actions.
- Budget approval for any corrective actions.
- The most recent results of compliance monitoring and auditing.
- Records from updated risk register.

2.3.4. The independent reviews shall take place at planned intervals and when significant incidents or significant changes to operations or risks occur.

GUIDANCE

- Independent reviews should take place at least annually, taking into account:
  - significant incidents, if any;
  - changes to the environment of operation;
  - changes to the threat landscape and cybersecurity legal and regulatory requirements; and
  - changes to the policy on the security of network and information systems and/or topic-specific policies.

EXAMPLES OF EVIDENCE

- Independent review reports documenting findings, recommendations and actions taken in response.
- Summaries of previous independent reviews, highlighting the scope and frequency.
- Records of significant incidents that occurred in the past year, along with any corresponding review or analysis documentation.
- Annual independent review plans or schedules that outline the scope of independent reviews and the specific measures being evaluated.

TIPS

GUIDANCE

- Make sure that the independent review process is approved by management bodies.
- Make sure that the results of the review are approved by management bodies.

EXAMPLES OF EVIDENCE

- Documented procedures approved by management bodies.
- Approval of the residual risks by management bodies.

Chapter 3

INCIDENT HANDLING

3. INCIDENT HANDLING

3.1 INCIDENT HANDLING POLICY

3.1.1. For the purpose of Article 21(2), point (b) of Directive (EU) 2022/2555, the relevant entities shall establish and implement an incident handling policy laying down the roles, responsibilities and procedures for detecting, analysing, containing or responding to, recovering from, documenting and reporting of incidents in a timely manner.

GUIDANCE

- Define clear objectives for the incident handling policy.
- Ensure the policy complies with relevant laws, regulations and industry standards ([17]).

EXAMPLES OF EVIDENCE

- Documented incident handling policy that contains, at least, the elements referred to in point 3.1.2 of the Annex to the regulation.
- Documented standards and/or good practices that are taken into consideration for this policy.

3.1.2. The policy referred to in point 3.1.1 shall be coherent with the business continuity and disaster recovery plan referred to in point 4.1. The policy shall include:

(a) a categorisation system for incidents that is consistent with the event assessment and classification carried out pursuant to point 3.4.1;

(b) effective communication plans including for escalation and reporting;

(c) assignment of roles to detect and appropriately respond to incidents to competent employees;

(d) documents to be used in the course of incident detection and response such as incident response manuals, escalation charts, contact lists and templates.

GUIDANCE

- Align the incident handling policy with the business continuity and disaster recovery plan (Annex to the regulation, point 4.1) by (indicative, non-exhaustive list):
  - ensuring that they aim to minimise disruptions, protect assets and ensure a swift return to normal operations;
  - identifying interfaces between the incident handling policy and business continuity management;
  - describing workflows which trigger business continuity (Annex to the regulation, points 4.1, 4.2 or 4.3) during an incident; and
  - developing scenarios that test the interaction between these processes and describe the result of this interaction in the incident handling policy.

([17]) In addition, consider the 'Incident response recommendations and considerations for cybersecurity risk management' from NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

- Set up a categorisation system for incidents, which refers to the scheme that the entity uses to identify the consequences and the priority of an incident, together with the criteria for categorising events as incidents ([18]). An indicative, non-exhaustive list of criteria might include one or more of the following:
    - impact on business operations,
    - data sensitivity in accordance with risk management,
    - legal and regulatory impact, including reporting timelines stemming from regulatory framework e.g. GDPR, national regulations,
    - scope and scale meaning the evaluation of how widespread the event is,
    - type of attack ([19]),
    - malicious software/vulnerability exploitation,
    - criticality of the systems affected,
    - incident containment urgency,
    - potential of data exfiltration or corruption, such as in the case of ransomware,
    - likelihood of recovery,
    - impact on human lives and safety and
    - other criteria on what constitutes a significant incident as per this regulation.
- Ensure that the incident handling policy refers to different types of incidents such as (indicative, non-exhaustive list):
    - system failures and loss of service availability;
    - malicious code;
    - denial of service;
    - errors;
    - breaches of confidentiality and integrity; and
    - misuse of network and information systems.
- Communicate the incident to relevant stakeholders and personnel according to a communication plan. The communication plan should consider the event reporting mechanism (Annex to the regulation, point 3.3) and may include (indicative, non-exhaustive list) the following:
    - purpose and scope of the plan,
    - roles and responsibilities for communication tasks,
    - list of internal and external stakeholders to be informed,
    - reporting timelines stemming from regulatory framework, e.g. GDPR, national regulations,
    - conditions and procedures for escalation of incidents,
    - channels to be used for communication (e.g. email, intranet, phone calls, social media, press releases),
    - channels of communication need to be tailored based on the target audience (that is internal, client or general public, etc.),
    - methods for stakeholders to provide feedback or ask questions and

([18]) The ISO/IEC 27035 series provides further guidance on incident management: ISO/IEC 27035-1:2023(en) Information technology – Information security incident management – Part 1: Principles and process. For the categorisation of incidents, please also consult the ENISA guidelines related to Article 23(9) summary reporting for the NIS2 Directive or information provided by the national computer security incident response teams (CSIRTs).

([19]) A cyberattack involves deliberate and malicious attempts to compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by or accessible via, network and information systems. The attack can be due to insider activity or external perpetrators.

- guidelines for when to communicate and the frequency of updates, along with pre-drafted message templates for various scenarios and the core messages to be communicated.
- Identify the necessary roles and responsibilities to be assigned for incident handling. The entities can use already established skills frameworks, for example the ECSF, to assist them in identifying the necessary skills and knowledge.

EXAMPLES OF EVIDENCE

- Cross references between the incident handling policy and the business continuity and disaster recovery plan, if available.
- Records of testing and drills that involve both incident handling and business continuity / disaster recovery.
- Interviews with key personnel involved in incident response, business continuity and disaster recovery.
- An incident categorisation system.
- Evidence that the incident handling policy is in place and communicated to employees.
- Evidence that a communication plan for incident handling is in place.
- Procedures for how to communicate the incident to relevant authorities and the computer security incident response team (CSIRT) are in place.
- Procedures for how to communicate the incident to customers or how and when to involve a supplier (if applicable).

3.1.3. The roles, responsibilities and procedures laid down in the policy shall be tested and reviewed and, where appropriate, updated at planned intervals and after significant incidents or significant changes to operations or risks.

GUIDANCE

- Consider one or more of the following to test the entity's incident handling policy (indicative, non-exhaustive list):
  - tabletop exercise,
  - simulation of an incident, preferably based on a selected attack scenario based on identified risks and the current threat landscape,
  - red team/blue team exercise and
  - past incident walk-through.
- Test the roles, responsibilities and procedures laid down in the policy at least annually.
- Review and update roles, responsibilities and procedures laid down in the policy at least annually, taking into account the following, in addition to the elements referred to in point 3.1.3 of the Annex to the regulation:
  - results from the policy tests,
  - changes to the threat landscape and cybersecurity legal and regulatory requirements and
  - changes to the policy on the security of network and information systems and/or topic-specific policies.

EXAMPLES OF EVIDENCE

- Periodic simulations and awareness raising activities to assess the readiness of personnel and the adequacy of the procedures.
- Incident handling policy testing plans or schedules.
- Incident handling policy review plans or schedules.
- Procedure updates (version history), if available.

TIPS

GUIDANCE

- Identify and consider all internal and external resources required in the event of an incident and ensure their availability at any time:
  - make sure that personnel are properly trained to handle and manage incidents;
  - identify and consider all external stakeholders (e.g. operators, technology suppliers, free and open source ([20]) project contacts, national competent authorities or CSIRTs) necessary for incident handling.
- Changes in the policy should be communicated to the relevant personnel.
- Ensure a clear overview of the various incident reporting obligations that the entity must fulfil under different reporting regimes.

EXAMPLES OF EVIDENCE

- Detailed procedures for the incident handling policy communicated to personnel as appropriate.
- A list of reporting obligations and deadlines, which may cover both legal and contractual obligations.

3.2 MONITORING AND LOGGING

3.2.1. The relevant entities shall lay down procedures and use tools to monitor and log activities on their network and information systems to detect events that could be considered as incidents and respond accordingly to mitigate the impact.

GUIDANCE

- Identify one or more objectives of monitoring and logging (indicative, non-exhaustive list):
  - threat detection,
  - compliance assurance,
  - incident response support,
  - performance optimisation,
  - anomaly detection,
  - monitor for new vulnerability reports issued for any free and open source software components ([21]) used by the entity,
  - data loss prevention,
  - forensic investigations support and
  - network health monitoring.
- Procedures should describe (indicative, non-exhaustive list):
  - objectives,
  - data for collection and relevant tools,
  - description of data algorithms and
  - mechanisms for notifying the relevant personnel.

([20]) Most software today builds on the rich foundation of infrastructure that has been provided freely by free and open source software (FOSS) projects and communities. In line with the approach to FOSS in Regulation (EU) 2024/2487, this document includes guidance on the responsible use of free and open source software in relevant sections, for example in sections 5.1 and 6.1.

([21]) Article 3(6) of the Cyber Resilience Act.

- Select tools that serve the objectives of monitoring and logging according to specific criteria (indicative, non-exhaustive list):
    - ease of use,
    - integration with the existing network and information system, including cross-border operations and the associated regulatory, security and performance considerations,
    - minimisation of manual intervention,
    - capability of collecting data from various sources, for example networks, systems and applications,
    - security features offered, for example encryption and access control and
    - costs and licencing.

EXAMPLES OF EVIDENCE

- Procedures in place.
- Tools in place.
- Configuration settings of the logging function that serve the identified objectives.
- Configuration settings of the logging function in line with documented standards and/or good practices.
- Safeguards to protect the confidentiality, integrity and availability of logs.

3.2.2. To the extent feasible, monitoring shall be automated and carried out either continuously or in periodic intervals, subject to business capabilities. The relevant entities shall implement their monitoring activities in a way which minimises false positives and false negatives.

GUIDANCE

- To minimise false positives and false negatives, to the extent feasible, consider one or more of the following (indicative, non-exhaustive list):
    - establish network traffic patterns;
    - use analytics and machine learning algorithms;
    - continuously update the automated monitoring tools to adapt to new threats and changes in the environment; and
    - fine-tune the parameters and thresholds based on the latest data and feedback.
- Where appropriate, ensure that all potential risks are properly covered by relevant use cases, for example use case for access to critical data, use case for data exfiltration or use case for ransomware infection, so that no critical threat goes undetected.

EXAMPLES OF EVIDENCE

- Acceptable log monitoring, collection, storage and analysis tools, in line with the state of the art.
- Security Incident and Event Management (SIEM) systems used to analyse data and identify deviations from established patterns.
- Endpoint detection and response (EDR) and Extended Detection and Response (XDR) tools in place.
- Mechanisms that aim to minimise false positives and false negatives are in place.
- Where appropriate, mapping use cases to potential risks to ensure comprehensive and effective monitoring.

3.2.3. Based on the procedures referred to in point 3.2.1., the relevant entities shall maintain, document and review logs. The relevant entities shall establish a list of assets to be subject to logging based on the results of the risk assessment carried out pursuant to point 2.1. Where appropriate, logs shall include:
(a) relevant outbound and inbound network traffic;
(b) creation, modification or deletion of users of the relevant entities' network and information systems and extension of the permissions;
(c) access to systems and applications;
(d) authentication-related events;
(e) all privileged access to systems and applications and activities performed by administrative accounts;
(f) access or changes to critical configuration and backup files;
(g) event logs and logs from security tools, such as antivirus, intrusion detection systems or firewalls;
(h) use of system resources, as well as their performance;
(i) physical access to facilities;
(j) access to and use of their network equipment and devices;
(k) activation, stopping and pausing of the various logs;
(l) environmental events.

GUIDANCE

- With regard to critical configuration, consider the settings and parameters that are vital for the proper functioning, security and performance of the entity's network and information system. These configurations are vital because any changes or misconfigurations might have a significant impact, including system outages, security vulnerabilities or reduced performance of the entity's network and information system.
- Consult the risk assessment results to determine which network traffic needs to be logged. For example, if certain assets are identified as high risk (e.g. due to being potentially vulnerable or crucial to the business operation) their inbound and outbound traffic should be logged for monitoring and analysis.

EXAMPLES OF EVIDENCE

- Samples of log files containing the elements referred to in point 3.2.3 of the Annex to the regulation.
- Samples of log files containing current and historical domain name system (DNS) and dynamic host configuration protocol (DHCP) logs.

3.2.4. The logs shall be regularly reviewed for any unusual or unwanted trends. Where appropriate, the relevant entities shall lay down appropriate values for alarm thresholds. If the laid down values for alarm threshold are exceeded, an alarm shall be triggered, where appropriate, automatically. The relevant entities shall ensure that, in case of an alarm, a qualified and appropriate response is initiated in a timely manner.

GUIDANCE

- Consider the use of anomaly detection or adaptive alarm thresholds to complement traditional static rules.
- Make sure that procedures are designed to detect network-based attacks based on anomalous inbound and outbound ingress or egress traffic patterns and/or denial of service (DoS) attacks, in a timely manner.

- Make sure that alarm thresholds, where appropriate, have been set in alignment with the results of the risk assessment carried out pursuant to point 2.1, covering at least the situations in point 3.2.3 of the Annex to the regulation. An indicative, non-exhaustive list of examples with thresholds ([22]) follows:
  - relevant outbound and inbound network traffic: traffic volume spikes exceeding 50% of normal traffic in a 10-minute period on a specific port;
  - access to systems and applications: three or more account lockouts within 15 minutes;
  - privileged access: two or more instances of privilege escalation (e.g. normal user to admin) within 24 hours ([23]);
  - antivirus: malware is detected on multiple endpoints within a short timeframe;
  - use of system resources: installations of unauthorised software within a short timeframe.

EXAMPLES OF EVIDENCE

- Regular reports that summarize log data and highlight any anomalies detected.
- Alarm thresholds set.
- Records from past alarm triggers when thresholds were exceeded.
- Existing workflows that trigger event reporting (section 3.3).

3.2.5. The relevant entities shall maintain and back up logs for a predefined period and shall protect them from unauthorised access or changes.

GUIDANCE

- Make sure that the log retention period is defined in accordance with business needs, the risk assessment results and legal requirements/obligations.
- The backup logs' maintenance period shouldn't be shorter than the logs' review period, referred to in point 3.2.4 of the Annex to the regulation.
- The retention period should be in line with what is referred to in point 4.2.2 (f) of the Annex to the regulation.
- Delete data when the retention period ends.
- Consider mechanisms to protect logs from unauthorised access or changes (indicative, non-exhaustive list):
  - encryption,
  - access control,
  - hashing (section 9.2) and
  - logging of all access and changes to log files.
- The access control should be in line with what is referred to in point 4.2.2 (d) of the Annex to the regulation.

EXAMPLES OF EVIDENCE

- A retention period is set.

([22]) The thresholds are subject to the operational environment. There are several assumptions about the environment that would need to be true for these controls/thresholds to be relevant. For certain entities, we expect that these entities will be under constant attack by bad actors and, accordingly, should be permitted to leverage continuous, automated and immediate responses.
([23]) Privileged access alarms shall distinguish between (a) administrative privilege assignment events (e.g. creation or promotion of accounts to privileged status) and (b) the use of existing privileged accounts by authorized personnel. The system shall generate an immediate alert upon detection of unauthorized or unexpected privilege assignments and a behavioural threshold alert (e.g. ≥2 privilege elevations within 24 hours) for monitoring legitimate administrative access patterns.

- The retention period is in line with what is referred to in point 4.2.2 (f) of the Annex to the regulation and is shorter than the logs' review period, referred to in point 3.2.4 of the Annex to the regulation.
- Log management is in place.
- Logs do not contain data about which retention periods have expired.
- Access control mechanisms are in place.
- Access control is in line with what is referred to in point 4.2.2 (d) of the Annex to the regulation.

3.2.6. To the extent feasible, the relevant entities shall ensure that all systems have synchronised time sources to be able to correlate logs between systems for event assessment. The relevant entities shall establish and keep a list of all assets that are being logged and ensure that monitoring and logging systems are redundant. The availability of the monitoring and logging systems shall be monitored independent of the systems they are monitoring.

GUIDANCE

- Consider the following for time synchronisation:
  - Utilize Network Time Protocol (NTP) servers or Precision Time Protocol (PTP) for accurate and reliable time synchronization ([24]).
  - Use authenticated NTP to prevent malicious entities from tampering with your time synchronization.
  - Configure a central time server within the entity ([25]). This server should synchronize with a reliable external time source and then distribute the time to all other systems within the network.
  - Use multiple time sources to avoid a single point of failure.
  - Plan how time synchronization is handled across on-premises systems (for example servers in a company's own data centre), cloud services, and software-as-a-service (SaaS) platforms - especially if the organization uses a hybrid environment (a mix of on-premises and cloud-based systems).
- Assets being logged should be marked as such in the asset inventory, in line with what is referred to in point 12.4 of the Annex to the regulation.
- Implement measures to protect log data against loss, including but not limited to redundant storage across multiple locations (e.g. cloud, secondary servers), retention of processed log events in structured systems and preservation of derived security insights (e.g. alerts, metrics) in line with what is referred to in point 4.2 of the Annex to the regulation. These complementary approaches ensure both data integrity and operational continuity in security monitoring and incident response.
- Deploy separate tools to monitor the capacity and availability of the entity's primary monitoring and logging systems.

EXAMPLES OF EVIDENCE

- Mechanisms for logs' time synchronisation.
- Mechanisms for logs' redundant storage.
- Logs from the activity of the tools that monitor the capacity and availability of the entity's primary monitoring and logging systems.

([24]) For public NTP servers, see https://ntp.org/.
([25]) Entity risk analysis should include definition on the stratum level required for the chosen sources of time synchronisation.

3.2.7. The procedures as well as the list of assets that are being logged shall be reviewed and, where appropriate, updated at regular intervals and after significant incidents.

GUIDANCE

- Determine the frequency of reviews based on the risk assessment results related to the criticality of the assets, ensuring that reviews are conducted at least annually.
- Include the testing of monitoring and logging procedures in security testing (section 6.5).
- Review a random sample of logs to verify that all the assets that should be subject to the log are actually considered.

EXAMPLES OF EVIDENCE

- Review plans or schedules.

TIPS

GUIDANCE

- In addition to the elements mentioned in point 3.2.3 of the Annex to the regulation, last login for every account should be logged.
- Document monitoring and logging procedures.
- Assess the frequency of monitoring activities to ensure they are sufficient to support risk-based security decisions for adequately protecting the entity's network and information systems.
- Make sure that personal data that are included in the logs is not processed unnecessarily. When required, an additional level of protection is deployed after performing a data protection impact assessment.
- Determine the log baselines in line with the needs and the capabilities of the business (indicative, non-exhaustive list):
  - structured or semi-structured, if possible, instead of unstructured format;
  - consistent data format in line with the selected tools and well-known standards, for example JavaScript Object Notation and extensible markup language (XML);
  - log level in line with the classification level of the asset being logged – the entity should assign a higher log level, for example 'error'/'fatal', to highly classified assets while the lower log levels, for example 'info'/'debug', should be used for assets with a lower classification; and
  - the standard for the timestamps, for example ISO-8601 ([26]), RFC 3339 ([27]) or RFC 9557 ([28]).
- Each log entry should contain necessary metadata such as (indicative, non-exhaustive list):
  - log level;
  - timestamp;
  - source identifier, for example the application or the device relevant to the entry; and
  - a unique identifier for the entry.
- Correlate data from different sources, if applicable.
- Select tools that monitor and protect end point devices.
- Select tools that can collect and analyse network traffic in real time to detect anomalies, data exfiltration and even the most advanced threats, while offering the option of automatic remediation.

([26]) ISO 8601-1:2019/Amd 1:2022 Date and time – Representations for information interchange, 2022 edition.
([27]) RFC3339, Date and time on the internet: Timestamps, July 2002, https://doi.org/10.17487/RFC3339.
([28]) RFC9557, Date and time on the internet: Timestamps with additional information, April 2024, https://doi.org/10.17487/RFC9557.

EXAMPLES OF EVIDENCE

- Documented procedures.
- Log baselines in place.
- Logs (samples) containing necessary metadata.
- EDR tools.
- Network detection and response (NDR) tools.

3.3 EVENT REPORTING

3.3.1. The relevant entities shall put in place a simple mechanism allowing their employees, suppliers and customers to report suspicious events.

GUIDANCE

- Define what constitutes a suspicious event based on criteria (indicative, non-exhaustive list):
  - if the confidentiality or the integrity or the availability of the network or the information system has been affected;
  - persistence, meaning whether the event is ongoing or not;
  - impact, for example. the number of assets (potentially) affected; and
  - compliance violation of a regulation or the entity's policies.
- Develop clear and concise guidelines for what information should be included in a report. Align this information with the information that might be submitted to the CSIRT or, where applicable to the competent authority, if the event is notified in accordance with the NIS2 Directive Articles 23 or 30. As good practice, the following should be reported as a minimum (indicative, non-exhaustive list):
  - date and time of the event,
  - description of the event,
  - any relevant screenshots, logs or other evidence,
  - contact information for follow-up if necessary.
- Provide multiple channels for reporting, such as email, a web form, a dedicated phone line or a mobile app. Ensure that these channels are easily accessible and intuitive to use.

EXAMPLES OF EVIDENCE

- Documented mechanism that outlines the process for reporting security events.
- Examples of templates for reporting ([29]).
- Personnel aware of the mechanism and who to contact if they notice something suspicious.
- Existence of multiple reporting channels such as email addresses, web forms, phone numbers or dedicated reporting portals.

([29]) Seek consistency with the reporting templates required by the national CSIRT or, where applicable, the competent authority.

3.3.2. The relevant entities shall, where appropriate, communicate the event reporting mechanism to their suppliers and customers and shall regularly train their employees how to use the mechanism.

GUIDANCE

- Make appropriate means for reporting available to personnel and the entity's suppliers and customers.
- Consider anonymous reporting to encourage individuals to report security events without fear of reprisal.
- Take into account legal obligations to report an incident to the competent authorities (and CSIRTs) in line with the NIS2 Directive Articles 23 and 30, including any obligations about when the incident should be reported.
- Regularly remind stakeholders of the reporting mechanism through email newsletters, posters and other communication channels.
- Conduct regular exercises or simulations to test the effectiveness of the reporting mechanism.

EXAMPLES OF EVIDENCE

- Evidence of past communications and event reporting.
- Documented procedures for communicating about events, describing (indicative, non-exhaustive list:
  - reasons/motivations for communicating or reporting (business reasons and legal reasons, etc.),
  - the type of events in scope,
  - the required content of communications,
  - notifications or reports,
  - the channels to be used and
  - the roles responsible for communicating, notifying and reporting.
- Training materials provided to employees, suppliers and customers regarding the reporting mechanism.
- Periodic simulations and awareness raising activities to assess the readiness of personnel and the adequacy of the mechanism for reporting an event.

TIPS

GUIDANCE

- Maintain a record of all reported events.
- Ensure compliance with other relevant regulations and laws regarding data privacy, confidentiality and incident reporting.
- Ask for legal advice, if necessary, to understand any legal implications of the reporting mechanism.
- Evaluate past communications and reporting about events.
- Review and update the reporting mechanism and the communication plans (Annex to the regulation, point 3.3), based on changes or past events.

EXAMPLES OF EVIDENCE

- Record of events and, for each event, the impact, cause, actions taken and lessons learnt.
- Summaries of previous reviews, if any.

3.4 EVENT ASSESSMENT AND CLASSIFICATION

3.4.1. The relevant entities shall assess suspicious events to determine whether they constitute incidents and, if so, determine their nature and severity.

GUIDANCE

- Use criteria to assess whether a suspicious event is an incident or not. The guidance in section 3.1.2 provides an indicative, non-exhaustive list of such criteria.
- Determine the nature and severity of the event based on a categorisation system referred to in point 3.1.2 (a) of the Annex to the regulation.

EXAMPLES OF EVIDENCE

- Defined criteria in place.
- A categorisation system referred to in point 3.1.2 (a) of the Annex to the regulation.

3.4.2. For the purpose of point 3.4.1, the relevant entities shall act in the following manner:
(a) carry out the assessment based on predefined criteria laid down in advance and on a triage to determine prioritisation of incident containment and eradication;
(b) assess the existence of recurring incidents as referred to in Article 4 of this Regulation on a quarterly basis;
(c) review the appropriate logs for the purposes of event assessment and classification;
(d) put in place a process for log correlation and analysis and
(e) reassess and reclassify events in case of new information becoming available or after analysis of previously available information.

GUIDANCE

- In the procedures defined in points 3.1.1 and 3.1.2 of the Annex to the regulation, include activities for assessing suspicious events to determine their nature and severity. These activities should include steps such as:
  - gathering relevant information and evidence related to the event.
  - analysing the potential impact on the entity's systems, data and operations.
  - determining the severity of the incident based on predefined criteria.
- Implement playbooks ([30]) or runbooks to guide initial assessment actions for common types of incidents, for example ransomware, phishing, data or device loss, or fire.
- Classify events based on their nature, severity and potential impact. Common classifications may include:
  - low, medium, high or critical severity;
  - incident types (e.g. malicious software infection or unauthorized access);
  - regulatory or compliance implications.
- Prioritise the event according to specific criteria, as defined in the categorisation system included in the incident handling policy referred to in point 3.1.2 of the Annex to the regulation.
- By performing root cause analysis ([31]), determine recurring instances ([32]) of an incident.

([30]) An example of good practice for such playbooks is the OASIS Collaborative Automated Course of Action Operations (CACAO) Security Playbooks Version Specification, v2.0, https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html.
([31]) More information on information security incident root cause analysis can be found in Forum of Incident Response and Security Teams, 'FIRST CSIRT services framework', Version 2.1, '6.2.4 Function: Information security incident root cause analysis', https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1#6-Service-Area-Information-Security-Incident-Management.
([32]) For the criteria on recurring incidents, see Article 4 of Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024.

    - Consider that the root cause of an incident may be challenging to determine during the early stages of incident handling, so the assessment of the existence of recurring incidents may be delayed.
- Review and correlate the logs in line with what is referred to in point 3.2 of the Annex to the regulation.
- Assess past events and their classification to improve processes, procedures and thresholds.

EXAMPLES OF EVIDENCE

- Documented procedures or guidelines related to event assessment, including steps for gathering information, analysing impact and determining severity.
- Existence of documented criteria or guidelines for prioritizing events based on severity and potential impact.
- Existence of a process for triaging incoming alerts or reports of suspicious events.
- Playbooks for common types of incidents.
- Periodic reviews of assessment and classification of past events to improve processes, procedures and thresholds.

TIPS

GUIDANCE

- Consider deploying SIEM, EDR, XDR or similar system that will allow and facilitate the correlation and analysis of data.
- Where possible, utilise automation to triage incoming alerts and prioritise them based on severity and potential impact.
- Integrate security events into the central SIEM or EDR/XDR solution, where available.
- Take into account the confidentiality of the data stored, especially when correlating and analysing log files, by (indicative, non-exhaustive list):
    - minimising data collected, meaning only collecting and analysing logs that fit the purpose – avoid retaining unnecessary personal or sensitive data;
    - anonymising or pseudonymising the collected data, when possible;
    - applying good security practices where appropriate and relevant, such as access control, encryption, regular audits and monitoring;
    - applying the data retention policy in alignment with GDPR requirements and regularly purging data that is no longer needed; and
    - considering data protection and relevant legal and compliance obligations other than the NIS2 Directive.

EXAMPLES OF EVIDENCE

- SIEM, EDR/XDR or similar system.
- Tools supporting incident triage.
- Measures to protect the security of information during log analysis and correlation.

3.5 INCIDENT RESPONSE

3.5.1. The relevant entities shall respond to incidents in accordance with documented procedures and in a timely manner.

GUIDANCE

- Establish a dedicated incident response team comprising employees with the necessary technical expertise and authority to respond effectively to incidents, where appropriate.
- Define roles and responsibilities within the incident response team, such as incident coordinators, analysts and communication liaisons, where appropriate.
- Take into account industry-recognised standards when developing the incident response procedures ([33]).
- Implement playbooks or runbooks to guide incident response actions for common types of incidents.

EXAMPLES OF EVIDENCE

- Assignment of roles within the incident response team.
- Documented standards and/or good practices that are taken into account.
- Playbooks or incident response plans for common types of incidents.

3.5.2. The incident response procedures shall include the following stages:
(a) incident containment, to prevent the consequences of the incident from spreading;
(b) eradication, to prevent the incident from continuing or reappearing,
(c) recovery from the incident, where necessary.

GUIDANCE

- Create incident response procedures outlining the steps referred to in point 3.5.2 of the Annex to the regulation.
- Ensure that the handling of cybersecurity incidents takes into account the entity's priorities and the impact of the incident.
    - Recognize and address potential conflicts between the following objectives during incident handling:
        - forensic activities – preserving and securing evidence for legal, compliance or investigative purposes,
        - incident response activities – mitigating and removing current threats to prevent further damage and
        - operational continuity – minimizing disruption to IT services and maintaining critical operations.
    - Where these objectives conflict, establish a clear decision-making process that:
        - prioritises based on the accepted risk tolerance levels, business impact and legal obligations,

([33]) In addition to those mentioned in the mapping table at the end of this section, consider the following:
- ISO/IEC 27035-1:2023, Information technology – Information security incident management, Part 1: Principles and process;
- ISO/IEC 27035-2:2023, Information technology – Information security incident management, Part 2: Guidelines to plan and prepare for incident response;
- NIST SP 800-61 Rev. 2, 'Computer security incident handling guide', https://csrc.nist.gov/pubs/sp/800/61/r2/final.

        - involves coordination between cybersecurity, legal/compliance and operational teams and
        - documents the rationale for prioritisation decisions to ensure transparency and accountability.
    - Develop incident response playbooks that incorporate decision making and escalation paths for managing trade-offs between evidence preservation, threat containment and operational continuity.
- Keep the management bodies informed.

EXAMPLES OF EVIDENCE

- Procedures for incident response, including types of incidents that could occur, objectives, roles and responsibilities. Detailed description, for each incident type, of how to manage the incident and when to escalate to management bodies (e.g. chief information security officer), etc.
- Records from resolution of conflicting objectives during response to past incidents.

3.5.3. The relevant entities shall establish communication plans and procedures:
(a) with the Computer Security Incident Response Teams (CSIRTs) or, where applicable, the competent authorities, related to incident notification;
(b) with relevant internal and external stakeholders.

GUIDANCE

- Ensure that the communication plan (Annex to the regulation, point 3.1.2) includes procedures for how to communicate the incident to the relevant authorities, the national CSIRT and internal and external stakeholders, including, where applicable, customers, direct suppliers, service providers and, if open source is used, contacts for free and open source software projects.
- Include contact information for key personnel, external stakeholders and relevant authorities.

EXAMPLES OF EVIDENCE

- Procedures for how to communicate the incident to the relevant authorities and the CSIRT.
- Procedures for how to communicate the incident to customers or how and when to involve a supplier (if applicable).

3.5.4. The relevant entities shall log incident response activities in accordance with the procedures referred to in point 3.2.1. and record evidence.

GUIDANCE

- Log incident response information which contains (indicative, non-exhaustive list):
    - time of detection, containment and eradication;
    - when the systems recovered;
    - indicators of compromise;
    - root cause;
    - actions taken during each phase namely, detection, containment and eradication;
    - assessment of the scope and the level of impact of the incident;
    - communications when responding to the incident;

- post incident lessons learnt and recommendations; and
- whether the CSIRT or the competent authority was notified of the incident according to the NIS2 Directive Articles 23 and 30.

EXAMPLES OF EVIDENCE

- Logs from incident response.
- Use of a system (e.g. SIEM, EDR/XDR or ticket system).

3.5.5. The relevant entities shall test at planned intervals their incident response procedures.

GUIDANCE

- Test the entity's incident response procedures at least annually.
- Test different types of incidents, for example ransomware, phishing, data breach and DoS.
- Ensure that test scenarios involve employees from different departments as well as external stakeholders, for example suppliers and service providers.
  - Where necessary, include management bodies in the tests so that they understand their role during an incident.
- Conduct post-test reviews for possible lessons learnt.
- Update the incident response procedures based on the lessons learnt from the test, if applicable.

EXAMPLES OF EVIDENCE

- Documented plans or schedules for future incident response tests.
- Records from tests of different types of incidents.

TIPS

GUIDANCE

- Issue instructions on how to respond to the most common types of incidents (ransomware, phishing, data breach, DoS, etc.) including containment, eradication and recovery steps.
- Include guidelines for preserving evidence and maintaining chain of custody to support forensic analysis and legal proceedings if necessary.
- Consider the use of automated solutions for incident response, for example security orchestration, automation and response technologies or similar systems.

EXAMPLES OF EVIDENCE

- Up-to-date incident response procedures based on tests conducted and/or change logs.

3.6 POST-INCIDENT REVIEWS

3.6.1. Where appropriate, the relevant entities shall carry out post-incident reviews after recovery from incidents. The post-incident reviews shall identify, where possible, the root cause of the incident and result in documented lessons learned to reduce the occurrence and consequences of future incidents.

GUIDANCE

- Conduct root cause analysis ([34]) and identify the root cause of the incident, where possible.
- Identify contributing factors and areas for improvement in incident detection, response and recovery processes.
- Investigate significant incidents and write final incident reports, including actions taken and recommendations to mitigate future occurrence of this type of incident.
- Document lessons learnt, accompanied by recommendations and their owners, based on logs from incident response referred to in point 3.5.4 of the Annex to the regulation.
- Share any relevant findings in the post-incident review with affected stakeholders, for example suppliers, service providers, free and open source component maintainers.

EXAMPLES OF EVIDENCE

- Results of root cause analysis.
- Individual reports of the handling of significant incidents.
- Documented lessons learnt from incidents.

3.6.2. The relevant entities shall ensure that post-incident reviews contribute to improving their approach to network and information security, to risk treatment measures and to incident handling, detection and response procedures.

GUIDANCE

- Analyse the post-incident review findings to identify gaps and weaknesses in the entity's network and information security status.
- Make sure that the identified gaps and weaknesses feed back to the risk assessment and risk treatment plan (Annex to the regulation, point 2.1).
- Assess whether existing risk treatment measures were effective in preventing or mitigating the incident.
- Document the findings and lessons learnt from each post-incident review comprehensively.
- Consider whether information security requirements have been met throughout the handling of a cybersecurity incident or whether measures may need to be taken to restore them (e.g. resetting passwords for emergency administrative access).

EXAMPLES OF EVIDENCE

- Post-incident review reports that detail findings, lessons learnt and recommendations for improvement following security incidents.
- Analysis, resolution and mitigation measures taken, communicated to all relevant personnel.
- Updated risk assessment and risk treatment plan, which includes findings of the post-incident reviews.

([34]) More information on information security incident root cause analysis can be found in Forum of Incident Response and Security Teams, 'FIRST CSIRT services framework', Version 2.1, '6.2.4 Function: Information security incident root cause analysis', https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1#6-Service-Area-Information-Security-Incident-Management.

3.6.3. The relevant entities shall review at planned intervals if incidents led to post-incident reviews.

GUIDANCE

- Conduct an annual review or a review after significant incidents, to determine if an incident has led to a post-incident review.

EXAMPLES OF EVIDENCE

- Documented plans or schedules for future reviews.

TIPS

GUIDANCE

- Determine the composition of the review team, including members from relevant departments such as IT, security, legal and management bodies.
- Review existing network and information security policies, topic-specific policies relevant to the incident, incident handling procedures and policy and incident response procedures in light of the lessons learnt from post-incident reviews.

EXAMPLES OF EVIDENCE

- Minutes of the post-incident review team.
- Evidence of updates to network and information security or topic-specific policies and procedures based on the lessons learnt from post-incident reviews.

BUSINESS CONTINUITY AND CRISIS MANAGEMENT

4. BUSINESS CONTINUITY AND CRISIS MANAGEMENT

4.1 BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

4.1.1. For the purpose of Article 21(2), point (c) of Directive (EU) 2022/2555, the relevant entities shall lay down and maintain a business continuity and disaster recovery plan to apply in the case of incidents.

GUIDANCE

- Take into account industry-recognised standards when developing the business continuity ([35]) and disaster recovery plan.
- Create a list of natural disasters (e.g. hurricane, fire, flooding) and other occurrences (e.g. human error) that could affect the services together with a list of disaster recovery capabilities (e.g. backups, tests, recovery objectives, etc.).

EXAMPLES OF EVIDENCE

- Business continuity plan.
- Disaster recovery plan.
- Business continuity and disaster recovery plans are in line with documented standards and/or good practices.
- List of natural and/or major disasters that could affect the services and a list of disaster recovery capabilities (either those available internally or provided by third parties).

4.1.2. The relevant entities' operations shall be restored according to the business continuity and disaster recovery plan. The plan shall be based on the results of the risk assessment carried out pursuant to point 2.1 and shall include, where appropriate, the following:

(a) purpose, scope and audience;

(b) roles and responsibilities;

(c) key contacts and (internal and external) communication channels;

(d) conditions for plan activation and deactivation;

(e) order of recovery for operations;

(f) recovery plans for specific operations, including recovery objectives;

(g) required resources, including backups and redundancies;

(h) restoring and resuming activities from temporary measures.

GUIDANCE

- Keep logs of activation and execution of the business continuity plan, including:

([35]) For example,
- ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements,
- ISO 22313:2020 - Security and resilience — Business continuity management systems — Guidance on the use of ISO 2230 and
- NIST SP 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems.

  - decisions taken;
  - steps followed; and
  - final recovery time.
- Determine the order of recovery based on criteria, including (indicative, non-exhaustive list):
  - the asset classification level;
  - the importance of the service for the entity;
  - dependencies (services or assets that are essential for others are restored first);
  - recovery objectives (Annex to the regulation, point 4.1.3);
  - resource availability; and
  - regulatory requirements.
- Conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support exists after business continuity plan activation.
- Consider primary and alternate telecommunications service providers, section 13.1, to properly maintain disaster recovery plans (for the services provided).
  - For remote work, employees handling critical operations should:
    - have access to backup internet solutions (e.g. mobile broadband, tethering capabilities) and
    - participate in regular testing of failover options, including VPN access and voice communications (e.g. VoIP or cloud telephony) over backup networks.
- Prepare for recovery and restoration of services after a disaster by identifying measures such as:
  - failover sites in other regions;
  - backups of data with high criticality to remote locations; and
  - tested restore procedures with regular validation cycles.
- Make sure that third party services (e.g. hot site) will be available in case of disaster, where appropriate.
- Implement advanced measures for disaster recovery capabilities, where appropriate, for example:
  - full redundancy;
  - failover mechanisms; and
  - alternative site.

EXAMPLES OF EVIDENCE

- Measures in place for dealing with disasters, such as failover sites in other regions and backups of data to remote locations.
- Up-to-date organisational structures widely communicated.
- Inventory of sectors and services essential for and/or dependent on the continuity of the network and service operation, and contingency plans for mitigating the impact related to dependent and interdependent sectors and services.

4.1.3. The relevant entities shall carry out a business impact analysis to assess the potential impact of severe disruptions to their business operations and shall, based on the results of the business impact analysis, establish continuity requirements for the network and information systems.

GUIDANCE

- Based on the results of the BIA [36] and risk assessment, the entity should establish appropriate recovery objectives, referred to in point 4.1.2 (f) of the Annex to the regulation (indicative, non-exhaustive list):
  - Recovery time objectives (RTOs) to determine the maximum amount of time allowed for the recovery of business resources and functions (e.g. information and communications technology (ICT) systems and processes, respectively) after a disaster occurs, for example maximum downtime of the entity's website, enterprise resource planning (ERP) system or email system.
  - Recovery point objective (RPO) to determine how much data it is acceptable for specific ICT activities or applications to lose. Typically, they are measured in maximum time needed to recover data without causing unacceptable, according to the risk assessment, damage to the entity's activities, for example maximum recovery time for an e-commerce website, an ERP system or an email server.
  - Service delivery objective (SDO) to determine the minimum level of performance that needs to be reached by business functions during the alternate processing mode. An indicative and non-exhaustive list of examples includes:
    - the percentage of inbound calls to be answered by a call centre within a specific timeframe;
    - the level of availability of ordering and payment systems of an e-commerce website within a specific timeframe;
    - the restoration time for accessing essential shared folders via a cloud file access system; and
    - the timeframe within which the full functionality of the remote work infrastructure is restored.
  - Maximum acceptable outage (MAO) or maximum tolerable period of disruption (MTPD) to determine the time it would take for the potential impacts of not providing a product/service or performing an activity to become unacceptable or significant, in accordance with the risk assessment. Typically they are longer than RTOs. MAOs focus on service availability while RPOs focus on data loss. An indicative and non-exhaustive list of examples:
    - the period of time beyond which the customer service would be severely impacted and reputation risk increases quickly;
    - the longest period of time that extended outage of an e-commerce website might result to major loss of sales and customer trust;
    - the longest period of time that shared access to project files may halt collaboration or decision-making in case that data is stored in cloud; and
    - the maximum acceptable outage for remote work infrastructure beyond which business functions are significantly impaired and productivity losses begin to escalate.
- RTOs, RPOs and SDOs may be used to determine backup and redundancy procedures.

(36) Consider the following standards: ISO/TS 22317:2021 and NIST special publication 800-34. For definitions of terms, refer to ISO 22300:2021.

- Document disaster recovery plan, taking into account:
  - the RTOs, RPOs and SDOs; and
  - compliance with applicable regulations and legislation.

EXAMPLES OF EVIDENCE

- Documented BIA with specific recovery objectives.
- Processes, procedures and measures to ensure the required level of continuity in disruptive situations.

4.1.4. The business continuity plan and disaster recovery plan shall be tested, reviewed and, where appropriate, updated at planned intervals and following significant incidents or significant changes to operations or risks. The relevant entities shall ensure that the plans incorporate lessons learnt from such tests.

GUIDANCE

- Test, review and, if necessary, update the business continuity and disaster recovery plans at least annually.
- Choose and combine method(s) to test the business continuity and disaster recovery plans, such as:
  - alternative locations for personnel;
  - disaster recovery locations – hot sites;
  - digital twins;
  - simulations;
  - table top exercises.
- Test business continuity and disaster recovery plans regularly, taking into account:
  - change logs;
  - past incidents; and
  - results of previous tests.
- Where appropriate, test the disaster recovery plan at an alternate processing site to:
  - familiarize related personnel with the facility and available resources; and
  - evaluate the capabilities of the alternate processing site to support operations.
- Test data centre infrastructure for:
  - availability;
  - auto failover;
  - power failover between power providers and/or power provider to backup (for example generators or batteries); and
  - resilience to maintain service to customers.
- Define full recovery and reconstitution of the information system to a known state as part of the disaster recovery plan testing.
- Update business continuity and disaster recovery plans and related measures based on:
  - change logs;
  - past incidents;
  - documented results of the continuity of operations test activities; and
  - records of individual training activities.
- Review change logs and documented results from past tests on business continuity and disaster recovery plans to ensure that the plans incorporate lessons learnt from such tests.
- Review and, if necessary, update roles and responsibilities.

- Review dependent third parties' disaster recovery plans to ensure that the plans meet entity's business continuity requirements.
- Communicate changes to business continuity and disaster recovery plans to related key personnel.

EXAMPLES OF EVIDENCE

- Documented plans or schedules for future tests.
- Records from previous tests, reviews and possible updates.
- Logs of activation and execution of business continuity and disaster recovery plans, including decisions taken, steps followed and final recovery time.
- Communications, for example emails, documents and intranet announcements, concerning changes to the business continuity and disaster recovery plans.
- Evidences that lessons learnt from past tests are incorporated into the plans, for example workflow changes and updated plans.

TIPS

GUIDANCE

- In addition to the elements referred to in point 4.1.2 of the Annex to the regulation, the business continuity plan might address:
  - management commitment;
  - coordination among organisational units;
  - communication plan;
  - compliance with laws;
  - metrics for measuring the successful implementation of the plan.
- Protect the business continuity and disaster recovery plans from unauthorized disclosure and modification.
- Ensure that business continuity and disaster recovery plans are easily accessible during a system outage. An indicative, non-exhaustive list of options to achieve this:
  - physical copies;
  - cloud storage;
  - external drives;
  - mobile access.
- Distribute copies of the business continuity plan to the related key personnel.
- Monitor the activation and execution of the business continuity plan registering successful and failed recovery times.
- Add a reference or a description / connection with the incident handling policy, plan and procedures into the business continuity plan.
- Coordinate the business continuity plan with the respective plans of external service providers to ensure that continuity requirements are satisfied
- Train key personnel involved in continuity operations.
- Set up procedures in regard to the appropriate communication channels with the (inter)national competent authorities, including disaster management organisations and disaster-relief teams.
- Regularly train the responsible personnel in disaster recovery operations.
- Implement contingency plans for systems based on scenarios.

- Monitor the activation and execution of contingency plans, registering successful and failed RTOs, RPOs and SDOs.
- Implement contingency plans for high criticality dependent and inter-dependent sectors and services.

EXAMPLES OF EVIDENCE

- Measures, for example encryption and access control, for protecting business continuity and disaster recovery plans from unauthorized disclosure and modification.
- Up-to-date organisational structures widely communicated.
- Decision process for activating contingency plans.
- Contingency plans for systems, including clear steps and procedures for common threats, triggers for activation, steps and defined RTOs, RPOs and SDOs.
- Logs of activation and execution of contingency plans, including decisions taken, steps followed and final recovery time.

4.2 BACKUP AND REDUNDANCY MANAGEMENT

4.2.1. The relevant entities shall maintain backup copies of data and provide sufficient available resources, including facilities, network and information systems and staff, to ensure an appropriate level of redundancy.

GUIDANCE

- Consider whether to invest in own redundancy or to engage third parties, for example cloud providers, to provide such redundancy, in alignment with the BIA (Annex to the regulation, point 4.1.3).

EXAMPLES OF EVIDENCE

- Backups are physically separated from the systems that generated them.
- If the service is offered by a third party, SLAs.

4.2.2. Based on the results of the risk assessment carried out pursuant to point 2.1 and the business continuity plan, the relevant entities shall lay down backup plans which include the following:

(a) recovery times;

(b) assurance that backup copies are complete and accurate, including configuration data and data stored in cloud computing service environment;

(c) storing backup copies (online or offline) in a safe location or locations, which are not in the same network as the system and are at sufficient distance to escape any damage from a disaster at the main site;

(d) appropriate physical and logical access controls to backup copies, in accordance with the asset classification level;

(e) restoring data from backup copies;

(f) retention periods based on business and regulatory requirements.

GUIDANCE

- Recovery times should not exceed the recovery objectives referred to in 4.1.2 (f) of the Annex to the regulation.
- Concerning retention periods consider what is referred to in point 3.2.5 of the Annex to the regulation.
- If an entity engages third parties to ensure an appropriate level of redundancy, it should be clearly decided whether it is the entity's responsibility to compile the backup plans or if the third parties have any involvement in the process.

EXAMPLES OF EVIDENCE

- Backup plans.
- Logs from backup software that show regular backups are being performed.
- Backups physically separated and with an appropriate level of protection, including encryption.
- Logs or reports confirming that one copy of the backup is stored off-site, such as in a cloud storage service or a remote data centre.
- Configuration settings of backup software to verify that it is set up to create copies of data and store them on different media.
- Clear and concise restoration procedures that cover all relevant systems and services.
- If applicable, settings of the cloud storage service to ensure it is configured to receive and store backup copies.

4.2.3. The relevant entities shall perform regular integrity checks on the backup copies.

GUIDANCE

- Check the integrity of the backup copies. An indicative, non-exhaustive list of good practices is the following:
    - use checksums or hashing algorithms to verify that the data in your backups matches the original data (section 9.2);
    - implement automated scripts to run these checks regularly, reducing the risk of human error;
    - schedule regular tests to restore data from backups to ensure they are complete, functional and validated by business users to confirm the accuracy and usability of the restored data;
    - test various recovery scenarios, including full system restores and individual file recoveries, to ensure all aspects of your backup system are reliable; and
    - consider using cloud storage solutions for off-site backups, which often include built-in integrity checks and redundancy.

EXAMPLES OF EVIDENCE

- Logs or reports showing that checksum or hashing algorithms are used.
- Settings in backup software or scripts that specify the use of checksums or hashing algorithms.
- Records of regular tests in which data is restored from backups.
- Evidence of tests of different recovery scenarios, including full system restores and individual file recoveries.
- Logs or reports from actual incidents in which recovery procedures were implemented (Annex to the regulation, points 3.2 and 3.5).
- If the service is offered by a third party, SLAs.

4.2.4. Based on the results of the risk assessment carried out pursuant to point 2.1 and the business continuity plan, the relevant entities shall ensure sufficient availability of resources by at least partial redundancy of the following:
(a) network and information systems;
(b) assets, including facilities, equipment and supplies;
(c) personnel with the necessary responsibility, authority and competence;
(d) appropriate communication channels.

GUIDANCE

- Define minimum resources needed to ensure at least partial redundancy for each of points (a), (b), (c) and (d). These may include the following:
    - network and information systems: one or more of the following (indicative, non-exhaustive list):
        - multiple internet service providers,
        - load balancing,
        - mirrored servers,
        - virtualisation,
        - redundant array of independent disks;
    - assets: one or more of the following (indicative, non-exhaustive list):
        - shared workspaces,
        - backup locations,
        - spare equipment,
        - multiple suppliers for the same categories of products;
    - personnel: one or more of the following (indicative, non-exhaustive list):
        - job rotation,
        - backup assignments,
        - emergency drills;
    - multiple communication platforms, for example social media, messaging apps and email; and
    - multiple methods to power a site, either through multiple electrical providers or with a combination of electrical providers and backup mechanisms, such as generators.

EXAMPLES OF EVIDENCE

- One or more of the above mechanisms are in place.

4.2.5. Where appropriate, the relevant entities shall ensure that monitoring and adjustment of resources, including facilities, systems and personnel, is duly informed by backup and redundancy requirements.

GUIDANCE

- Decisions about resource allocation and adjustments should be guided by the need for backups and redundancy. To this end, the entity might consider one or more of the following (indicative, non-exhaustive list):
    - prioritisation of resources based on the results of the risk analysis;
    - partial redundancy;
    - diverse backup locations; and
    - continuous monitoring of the resources where redundancy is necessary.

EXAMPLES OF EVIDENCE

- Evidence of elements referred to in point 4.2.4 of the Annex to the regulation.
- Evidence from periodic simulations and awareness raising activities to assess the readiness of personnel and the adequacy of the procedures.

4.2.6. The relevant entities shall carry out regular testing of the recovery of backup copies and redundancies to ensure that, in recovery conditions, they can be relied upon and cover the copies, processes and knowledge to perform an effective recovery. The relevant entities shall document the results of the tests and, where needed, take corrective action.

GUIDANCE

- Tailor the frequency of the backup checks to the data criticality based on the risk assessment (section 2.1). As an example:
  - Data with high criticality might be checked on a weekly basis.
  - Data with moderate and low criticality might be checked on a monthly basis.
  - Significant changes should be checked immediately after the change.
- Make sure that the issues and lessons learnt from exercises are addressed by the responsible people and that the relevant processes and systems are updated accordingly.
- Involve suppliers and other third parties, such as business partners or customers in tests.

EXAMPLES OF EVIDENCE

- Reports/logs of regular testing of backup status, processes and procedures.
- Test programme for backup plans, including types of contingencies, frequency, roles and responsibilities, templates and procedures for conducting tests, and templates for post-test reports.
- Reports of past tests of backup and contingency plans.
- Reports about tests and drills showing the execution of the plans, including evidence that recovery times were met and lessons learnt from the tests.
- Issues and lessons learnt from past tests addressed by the responsible people.
- Updated test plans, review comments and/or change logs.
- Input from suppliers and other third parties involved about how to improve test scenarios.

TIPS

GUIDANCE

- Protect backup and restoration hardware and software.
- Ensure that encrypted backups remain accessible by securely maintaining the associated encryption keys. Encryption keys should be stored separately from the backup data to prevent unauthorized access and ensure recoverability.
- Before systems or configurations are restored, a ‘patient zero ([37])’ may need to be identified so that the restoration does not restore any vulnerabilities or infections that have sometimes been cleaned up.

([37]) This term is usually used to identify the first system affected by an attack.

- Consider the 3-2-1 backup rule:
  - keep **three** copies of the data (the original plus two backups),
  - on **two** different types of storage media (e.g. hard drives, cloud storage),
  - with **one** copy stored offsite.
- Ensure the integrity of backups, that is, prevent any modification or deletion, such as ransomware encryption or tampering, within a defined retention period. Ways to ensure this include (indicative, non-exhaustive list):
  - malware and ransomware scanning of backups before backups are stored;
  - use of immutable backups;
  - offline storage of backups.
- Integrate business continuity and disaster recovery plans with incident response (Annex to the regulation, point 3.5) and crisis management processes (Annex to the regulation, point 4.3).
- When available cloud services:
  - backups will be replicated across multiple availability zones or stored in an alternate region to ensure resilience against zone-level failures;
  - will be configured with cross-zone replication to minimise downtime;
  - all backup data will be encrypted at rest using cloud-native key management systems and encrypted during transfer using TLS 1.2+;
  - regular backup testing will be performed to validate cross-zone recovery capabilities.

EXAMPLES OF EVIDENCE

- Measures in place to protect backup and restoration hardware and software, for example physical access controls, surveillance systems, encryption, integrity checks and failover mechanisms.
- Review of the backup plan which mentions the 3-2-1 rule.
- Logs from backup software that show regular backups are being performed.
- Configuration settings of backup software to verify that it is set up to create three copies of data and store them on different media.
- If applicable, settings of the cloud storage service ensuring it is configured to receive and store backup copies.

4.3 CRISIS MANAGEMENT

4.3.1. The relevant entities shall put in place a process for crisis management.

GUIDANCE

- Take into account industry-recognised standards when developing the crisis management process ([38]).
  - Be aware that each crisis may be different and further analysis may be required on an ad hoc basis.
  - Consider the various aspects (e.g. technical, operational, communication and remediation) of crisis management, including processes, roles and responsibilities.

([38]) Additionally, consider:
- ISO 22361:2022, Security and resilience – Crisis management – Guidelines;
- ENISA Best Practices for Cyber Crisis Management, https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management;
- NIST Special Publication 800-61 Revision 2.

- Because the escalation of an incident to crisis status depends on an entity's risk appetite and incident handling capabilities, the entity should define criteria on when a crisis is declared ([39]). This may refer to incidents that cause serious impact, beyond a certain threshold of tolerance. These criteria may include the following (indicative and non-exhaustive list):
  - the incident poses significant risk to critical assets or operations with high criticality, for example high-severity incidents (e.g. data breaches involving sensitive information);
  - the incident disrupts business operations significantly, for example prolonged downtime, widespread loss of services or significant impact on customer service;
  - the breadth of the incident, that is, whether it affects multiple systems, departments or geographic locations, indicating a wider threat;
  - the potential impact on the entity's reputation – incidents that could lead to public scrutiny or loss of customer trust should be escalated;
  - the potential impact of the cybersecurity incident on the confidentiality, integrity, authenticity and availability of data;
  - the sophistication and motivations of the threat actors involved. Incidents linked to advanced persistent threats or organised cybercrime may require a higher-level response, beyond the capabilities of the entity;
  - the potential to escalate further (e.g. if vulnerabilities could be exploited again or if malware is spreading).

EXAMPLES OF EVIDENCE

- Crisis management process is in line with documented standards and/or good practices.

4.3.2. The relevant entities shall ensure that the crisis management process addresses at least the following elements:
(a) roles and responsibilities for personnel and, where appropriate, suppliers and service providers, specifying the allocation of roles in crisis situations, including specific steps to follow;
(b) appropriate communication means between the relevant entities and relevant competent authorities;
(c) application of appropriate measures to ensure the maintenance of network and information system security in crisis situations.
For the purpose of point (b), the flow of information between the relevant entities and relevant competent authorities shall include both obligatory communications, such as incident reports and related timelines and non-obligatory communications.

GUIDANCE

- For crisis communication, consider (indicative, non-exhaustive list):
  - legal obligations for communication, such as timing of communication, in particular referring to requirements for notification;
  - how information will be disseminated to internal and external stakeholders (employees, customers, direct suppliers and service providers, emergency services, etc.) during a crisis;
  - templates for communication;
  - communication channels to be used for each type of stakeholder, considering that:

([39]) According to ISO 22361, a crisis is an 'abnormal or extraordinary event or situation which threatens an organisation or community and requires a strategic, adaptive and timely response in order to preserve its viability and integrity'.

        - internal and external stakeholders may use different communication channels;
        - normal communication channels might not be safe in crisis mode;
        - channels used to notify and communicate with competent authorities should also be indicated;
    - up-to-date contact information for internal and external stakeholders.

EXAMPLES OF EVIDENCE

- Documented crisis management process.
- List of members of the crisis management team, including their roles, contact information and alternatives.

4.3.3. The relevant entities shall implement a process for managing and making use of information received from the CSIRTs or, where applicable, the competent authorities, concerning incidents, vulnerabilities, threats or possible mitigation measures.

GUIDANCE

- Implement a process for managing and making use of information received from the CSIRTs. Consider the following steps (indicative, non-exhaustive list):
    - designate a point of contact with the CSIRT;
    - ensure that the point of contact has sufficient knowledge concerning incidents and threat intelligence.
    - classify incoming information into categories such as incidents, vulnerabilities, threats and mitigation measures.
    - assign priority levels based on severity and potential impact on the entity, if the information is relevant or applicable
    - have the CSIRT contact point review the information for relevance and urgency.
    - validate information against internal logs, threat intelligence feeds and existing security policies.
    - for vulnerabilities and threats, if applicable, collaborate with relevant teams (IT, security, operations) to develop a mitigation strategy;
    - update or create incident response plans based on the nature of the threats or incidents reported in accordance with point 3.5 of the Annex to the regulation.
    - where appropriate, implement the mitigation measures and communicate with the relevant stakeholders in accordance with point 3.5 of the Annex to the regulation.
    - share insights and feedback on incidents and mitigations with the CSIRT on a voluntary basis.

EXAMPLES OF EVIDENCE

- Previous communications with CSIRTs or, where applicable, the competent authorities, for example emails, correspondence and meeting minutes.
- Evidences that the point of contact has sufficient knowledge concerning incidents and threat intelligence.

4.3.4. The relevant entities shall test, review and, where appropriate, update the crisis management plan on a regular basis or following significant incidents or significant changes to operations or risks.

GUIDANCE

- Test the crisis management process annually.

- Test the crisis management process through, for example, an exercise or simulation, by (indicative, non-exhaustive list):
  - taking into account past crisis situations;
  - comparing the results of the tests to the objectives defined, for instance the recovery objectives in point 4.1.2 (f) of the Annex to the regulation (e.g. RTOs, RPOs and SDOs); and
  - using the results of the comparison to update and improve the crisis management procedure.
- Review and update, if necessary, the crisis management process after a test or following significant incidents or significant changes to operations or risks.
- Review and update the policy on the security of network and information systems and crisis management organisational measures after a test or following significant incidents or significant changes to operations or risks.

EXAMPLES OF EVIDENCE

- Documentation showing how crisis management integrates with the entity's incident response plans (Annex to the regulation, point 3.5), particularly for ICT-related incidents.
- Documents identifying any previous crises and assessing their likelihood of recurrence and potential impact on business operations.
- Documentation of previous crisis management tests, including the scenarios tested, participants involved and outcomes.
- After-action reports or evaluations from crisis management tests, identifying strengths, weaknesses and areas for improvement.
- Records of internal or external reviews and audits of the crisis management plan, including any findings and corrective actions taken.

TIPS

GUIDANCE

- Management bodies should approve the crisis management process and, where appropriate, their roles and responsibilities during a crisis should be defined.
- In addition to the elements referred to in point 4.3.2 of the Annex to the regulation the crisis management process might identify (indicative, non-exhaustive list):
  - procedures for declaring a crisis;
  - activation of the crisis management team;
  - escalation paths;
  - emergency procedures, which describe the actions in the event of a crisis; and
  - fall back procedures that describe the actions to be taken to protect essential activities or support services (e.g. alternative temporary locations for bringing the process back to normal operation, recovery or restoration).

EXAMPLES OF EVIDENCE

- Inventory of resources required for crisis management, including backup systems, alternative communication tools and emergency supplies.
- Approved crisis management process.
- A crisis communication plan documented and approved by the management bodies in place and communicated to all personnel. In addition to the elements referred to in point 4.3.2 of the Annex to the

regulation and the elements of the above guidance, the plan includes at least (indicative, non-exhaustive list):

  - how information will be disseminated to stakeholders during a crisis;
  - templates for communication; and
  - up-to-date contact information for internal and external stakeholders, including employees, customers, suppliers and emergency services.

- Evidence that personnel are aware of the processes and who to contact in the event of a crisis.
- Records from periodic simulations and awareness raising activities to assess the readiness of personnel and the adequacy of the procedures for managing a crisis.

SUPPLY CHAIN SECURITY

5. SUPPLY CHAIN SECURITY

5.1 SUPPLY CHAIN SECURITY POLICY

5.1.1. For the purpose of Article 21(2), point (d) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a supply chain security policy which governs the relations with their direct suppliers and service providers to mitigate the identified risks to the security of network and information systems. In the supply chain security policy, the relevant entities shall identify their role in the supply chain and communicate it to their direct suppliers and service providers.

GUIDANCE

- Take into account industry-recognised standards or good practices when developing the supply chain policy ([40]).
- The role of a supplier or service provider might be one or more of the following ([41]):
  - ICT supplier (including software and hardware supplier),
  - Manufacturer,
  - managed service provider,
  - managed security service provider and
  - cloud computing provider.
- In the case of free and open source software (FOSS), communities and projects that openly develop, maintain and distribute software may not be considered direct suppliers or service providers where no contractual relationship exists between the relevant entity and the open source project, beyond adherence to a standardised copyright licence, or where the contractual relationship is with an open source software steward (Regulation 2024/2847, Article 3(14) 'provides support on a sustained basis for the development and ensures the viability of those products').

EXAMPLES OF EVIDENCE

- Supply chain security policy in place and is in line with industry-recognised standards and/or good practices.
- Evidence (e.g. email, contract or announcements) of the communication of the role of the entity to the direct suppliers and service providers, where possible.

5.1.2. As part of the supply chain security policy referred to in point 5.1.1, the relevant entities shall lay down criteria to select and contract suppliers and service providers. Those criteria shall include the following:
(a) the cybersecurity practices of the suppliers and service providers, including their secure development procedures;

([40]) In addition, consider the following:
- ISO/IEC 27036-1:2021, Cybersecurity – Supplier relationships Part 1: Overview and concepts;
- ISO/IEC 27036-2:2022, Cybersecurity – Supplier relationships Part 2: Requirements;
- NIST SP 800-161 Rev. 1, 'Cybersecurity supply chain risk management practices for systems and organizations', https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final;
- ENISA, *Good Practices for Supply Chain Cybersecurity*, https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity.

([41]) The list aligns with the draft EU ICT Supply Chain Toolbox from the NIS Cooperation Group workstream on supply chain, as of February 2025.

(b) the ability of the suppliers and service providers to meet cybersecurity specifications set by the relevant entities;
(c) the overall quality and resilience of ICT products and ICT services and the cybersecurity risk-management measures embedded in them, including the risks and classification level of the ICT products and ICT services;
(d) the ability of the relevant entities to diversify sources of supply and limit vendor lock-in, where applicable.

GUIDANCE

- Consider criteria such as:
  - the legal jurisdiction of the supplier or service provider, for example whether the supplier is regulated under the NIS2 Directive or the Cyber Resilience Act and in which jurisdiction(s);
  - if available, compliance statements from the supplier in relation to the NIS2 Directive;
  - the corporate ownership of the supplier or service provider;
  - the supplier's or service provider's ability to ensure supply (e.g. size, reliance on other suppliers or service providers and degree of control over its own supply chain);
  - the cybersecurity practices of the supplier or service provider, and whether adequate prioritisation is given to cybersecurity practices, attested by:
    - industry standard certifications for cybersecurity;
    - vendor risk-management software reports or other provider assessment reports (e.g. Standardized Information Gathering, vendor security assessment or consensus assessment initiative questionnaire), if available;
  - notices or advice issued by national authorities on the selection of suppliers or service providers, if available;
  - the sensitivity of the use of the products and services acquired;
  - the supplier or service provider's history in relation to cybersecurity events and breaches;
  - the possibility of vendor lock-in, if the supplier or service provider is selected. Parameters to consider are the use of open and interoperable standards, the use of open data formats, existing contracts with the supplier or service provider, the use of proprietary software features, etc.

EXAMPLES OF EVIDENCE

- A policy containing the elements referred to in point 5.1.2 of the Annex to the regulation.

5.1.3. When establishing their supply chain security policy, relevant entities shall take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of Directive (EU) 2022/2555, where applicable.

GUIDANCE

- Take into account any recommendations or guidance on supply chain security, published by the NIS Cooperation Group, established by the NIS2 Directive, Article 14 ([42]) and by the national competent authorities.

([42]) 'NIS Cooperation Group', https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.

EXAMPLES OF EVIDENCE

- Evidence that scenarios and the recommendations of the NIS Cooperation Group have been taken into account in the supply chain policy, relevant to the entity's business objectives.

5.1.4. Based on the supply chain security policy and taking into account the results of the risk assessment carried out in accordance with point 2.1. of this Annex, the relevant entities shall ensure that their contracts with the suppliers and service providers specify, where appropriate through service level agreements, the following, where appropriate:
(a) cybersecurity requirements for the suppliers or service providers, including requirements as regards the security in acquisition of ICT services or ICT products set out in point 6.1.;
(b) requirements regarding awareness, skills and training and where appropriate certifications, required from the suppliers' or service providers' employees;
(c) requirements regarding the verification of the background of the suppliers' and service providers' employees;
(d) an obligation on suppliers and service providers to notify, without undue delay, the relevant entities of incidents that present a risk to the security of the network and information systems of those entities;
(e) the right to audit or right to receive audit reports;
(f) an obligation on suppliers and service providers to handle vulnerabilities that present a risk to the security of the network and information systems of the relevant entities;
(g) requirements regarding subcontracting and, where the relevant entities allow subcontracting, cybersecurity requirements for subcontractors in accordance with the cybersecurity requirements referred to in point (a);
(h) obligations on the suppliers and service providers at the termination of the contract, such as retrieval and disposal of the information obtained by the suppliers and service providers in the exercise of their tasks.

GUIDANCE

- Ensure that, in all relevant new and renewed contracts, the requirements from point 5.1.4 of the Annex to the regulation are included.
- When dealing with large suppliers and service providers consider one or more of the following measures (indicative, non-exhaustive list):
  - collective bargaining by teaming up with similar size organisations for purchasing products or services in bulk;
  - representation by an association of which the entity is a member of;
  - legal advice for reviewing and negotiating a contract;
  - negotiating specific clauses such as exit, pricing and SLAs ([43]);
  - suppliers that publicly publish their security, privacy or reliability commitments;
  - providers with standard certifications (e.g. ISO 27001, SOC 2);
  - trusted platforms or marketplaces that vet suppliers (e.g. app stores, SaaS directories, partner networks);
  - contract templates or free legal checklists from small business associations, NGOs or government sites;
  - tools/services that allow easy data export, monthly payments or no lock-in;
  - avoiding long-term commitments or vendor lock-in without clear exit strategies; and

([43]) The entity remains fully accountable for the integrity, availability and confidentiality of services provided by suppliers. SLAs must be clearly defined, actively managed and aligned with the entity's business continuity, security and compliance obligations.

- a short list of alternatives in case the supplier becomes unavailable.

EXAMPLES OF EVIDENCE

- Contracts that contain the elements referred to in point 5.1.4 of the Annex to the regulation.

5.1.5. The relevant entities shall take into account the elements referred to in point 5.1.2 and 5.1.3. as part of the selection process of new suppliers and service providers, as well as part of the procurement process referred to in point 6.1.

GUIDANCE

- Perform a risk analysis before entering into any agreement with suppliers and service providers related to information security, taking into account the elements referred to in point 5.1.2 and 5.1.3, where appropriate ([44]).

EXAMPLES OF EVIDENCE

- Evidence that contracts with new suppliers and service providers or the procurement guidelines take into account the elements referred to in points 5.1.2 and 5.1.3.
- Comparison between selected contracts and the associated tenders to check whether the secure acquisition of ICT systems, products and service processes and particularly the elements referred to in point 6.1.2 of the Annex to the regulation, are taken into consideration.
- Risk analysis results from supplier and service provider evaluations.

5.1.6. The relevant entities shall review the supply chain security policy and monitor, evaluate and, where necessary, act upon changes in the cybersecurity practices of suppliers and service providers, at planned intervals and when significant changes to operations or risks or significant incidents related to the provision of ICT services or having impact on the security of the ICT products from suppliers and service providers occur.

GUIDANCE

- Review the supply chain policy at least annually.
- Create and maintain a process to monitor suppliers and service providers over the life cycle.

EXAMPLES OF EVIDENCE

- Supply chain policy review plans or schedules.
- Records from previous reviews.
- List of security incidents related to or caused by engagement with a supplier or service provider.
- Evidence that the policy was reviewed and possibly updated, after significant changes to operations or risks or significant incidents related to the provision of ICT services or having an impact on the security of the ICT products from suppliers and service providers.
- Evidence from evaluations of suppliers and service providers.

([44]) For example, for procuring security services or for recurring purchases in large quantities.

5.1.7. For the purpose of point 5.1.6., the relevant entities shall:

(a) regularly monitor reports on the implementation of the service level agreements, where applicable;

(b) review incidents related to ICT products and ICT services from suppliers and service providers;

(c) assess the need for unscheduled reviews and document the findings in a comprehensible manner;

(d) analyse the risks presented by changes related to ICT products and ICT services from suppliers and service providers and, where appropriate, take mitigating measures in a timely manner.

GUIDANCE

- Set up a regular review (e.g. as part of a regular supplier meeting) and follow up on deviations from the agreed SLAs.
- Define and assign responsibilities regarding maintenance, operation and ownership of assets.
- Make sure that monitoring encompasses periodic reassessment of supplier and service provider compliance, and monitor supplier and service provider release notes.
- Periodically ensure that product configuration is aligned with vendor recommendations, with increasing frequency as products age.
- Keep track of security incidents related to or caused by suppliers and service providers as they might trigger an unscheduled review of the suppliers and service providers. Other circumstances for such an unscheduled review include to suppliers and service providers (indicative, non-exhaustive list):
    - material changes in their operations;
    - changes in their risk exposure;
    - failure to meet their contractual obligations; and
    - emergence of new threats or vulnerabilities affecting the provided ICT products or services.
- Monitoring frequency should be aligned with supply chain policy (Annex to the regulation, point 5.1.1) and the review of the secure acquisition of ICT services, systems or products processes (Annex to the regulation, point 6.1.3).

EXAMPLES OF EVIDENCE

- Records showing that service levels are monitored in accordance with established SLA).
- Incident response records which confirm whether the entity takes into account incidents related to ICT services, systems or products from suppliers and service providers;
- Evidence that signed contracts with third parties (e.g. contractors and suppliers) are in line with the policy on the security of network and information systems, for example contractual clauses, references to key security-relevant roles and responsibilities, and requirements for the contractor to report incidents.
- Supplier and service provider exit process, meaning documentation outlining how the entity manages the exit of suppliers and service providers. This includes transitioning services, data and access rights when terminating a supplier and service provider relationship.
- List of security incidents related to or caused by engagement with third parties.

TIPS

GUIDANCE

- In addition to the elements referred to point 5.1.4 of the Annex to the regulation, consider the following additional elements for contract clauses (indicative, non-exhaustive list):
    - a clear and complete description of ICT products and services;

    - service level descriptions, including uptime guarantees or target service levels, response times for service issues and updates to the service level descriptions thereof;
    - locations (regions or countries) where the ICT products are to be produced and ICT services are to be provided and where data is to be processed, including the storage location and the requirement for the supplier and service provider to notify the entity in advance if it envisages changing such locations;
    - provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;
    - non-disclosure agreements;
    - obligations on the suppliers and service providers, such as retrieval and disposal of the information obtained by the suppliers and service providers in the exercise of their tasks, in the event of the insolvency, resolution, termination or discontinuation of the business operations of the supplier or service provider;
    - obligations of the supplier or service provider to provide assistance to the entity at no additional cost or at a cost that is determined *ex ante*, in the event of a cyber incident that presents a risk and was caused by the ICT product or the ICT service contracted;
    - roles and responsibilities;
    - contacts and reporting lines;
    - the obligation of the supplier or service provider to fully cooperate with the competent authorities;
    - termination rights and related minimum notice periods for the termination of the contractual arrangements;
    - notice periods and reporting obligations of the supplier or service provider to the entity, including notification of any development that might have a material impact on the supplier's or service provider's ability to effectively provide the ICT products or services in line with agreed service levels;
    - the right to audit by the entity or an appointed third party and by the competent authority and the obligation of the supplier and the service provider to fully cooperate during onsite inspections and audits performed by competent authorities and the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;
    - exit strategies, in particular the establishment of a mandatory adequate transition period, provisions on intellectual property and responsibilities of the supplier during the exit period, for example to provide relevant documentation and historical logs.
- In addition to the elements referred to in point 5.1.5 of the Annex to the regulation, consider the following (indicative, non-exhaustive list):
    - country-specific information (e.g. threat assessment from national security services), if available;
    - restrictions or exclusions posed by a relevant national authority, for example equipment with high criticality for the entity or for high-risk suppliers;
    - information stemming from known incidents or cyber threat intelligence; and
    - the characteristics of each supplier, such as the quality of its security practices, the legal framework and the level of transparency.
- Make sure that secure decommissioning service providers consider issues such as deactivating user and service accounts, terminating data flows and ensuring secure disposal of the entity's data within supplier or service provider systems.

- Awareness training regarding rules of engagement and behaviour should be delivered to the entity's and the suppliers or service providers' personnel, where appropriate, based on the level of access to the entity's assets and information assets.
- Include relevant personnel of suppliers and service providers and their relevant responsibilities, in crisis management tests, where appropriate.
- Make sure that contracts with suppliers and service providers are in line with the policy on the security of network and information systems.
- When implementing a supply chain security policy, consider the following elements regarding the use of free and open source software (FOSS) supply chain:
  - When using FOSS without purchasing a related software product or entering into a service agreement for development with the originator of the FOSS, obligations for compliance cannot be imposed beyond the adherence to the terms of the open source software licence ([45]).
  - Consider supporting the communities developing and maintaining FOSS and invest in a mutually beneficial relationship with them. Where effective, this could involve relationships with the relevant OSS steward that 'provid[es] support on a sustained basis for the development and ensures the viability of those products' ([46]). Such a relationship should not qualify the steward as a direct supplier or service provider, as imposing technical or methodological requirements might not be appropriate, applicable or feasible considering their role.
  - Consider steps to mitigate the identified risks to the security of network and information systems as it relates to free and open source software dependencies:
    - before integrating free and open source components, require the direct supplier or service provider to conduct a risk assessment and communicate the results to understand potential vulnerabilities and their impact on the entity's systems;
      - where feasible, the risk assessment should be done in coordination with its open source project or associated OSS Steward, at the expense of the supplier or service provider using the component and in such a way that subsequent risk assessments done by third parties benefit from this work;
    - require suppliers or service providers to provide evidence of their engagement with the OSS community to ascertain whether adequate resources are available to support sustainable maintenance efforts and contribute such resources where appropriate, including to guarantee future availability of security patches;
    - ensure that free and open source components are regularly updated by the supplier or the service provider to address all known and patched security vulnerabilities;

([45]) OSS, also known as free software or FOSS, guarantees its users the essential four freedoms: use, study, share and improve. OSS can be used for any purpose and is free of restrictions such as licence expiry or geographic limitations. Its software code can be studied by anyone, without non-disclosure agreements or similar restrictions. It can be shared and copied at virtually no cost. It be modified by anyone, and these improvements can be shared publicly. The absence or weakening of at least one of these freedoms means an application is proprietary, so non-OSS. The four freedoms are given by a software licence. Software licences define the conditions under which a programme can be used and reused. For it to be free software, the licence text must contain at least the four freedoms. The Free Software Foundation and the Open Source Initiative maintain lists of reviewed and approved licences. An application can usually not be considered OSS if its licence does not appear in one of these lists.
([46]) Regulation (EU) 2024/2847, Art. 3(14).

  - require the supplier or service provider to perform regular code reviews and security testing on free and open source components to identify and address any security issues ([47]);
  - require the supplier or service provider to provide information on tools to manage software dependencies (e.g. Dependabot, Yarn, Gradle and Pip) and ensure that all components and their dependencies are secure and up to date;
  - require the supplier or service provider to provide clear documentation and policies for using free and open source components, including guidelines for evaluation and integration, along with evidence of efforts to ensure the sustainable maintenance of their dependencies by nurturing the open source projects they rely on, such as by referencing their public (code) contributions.
- Engage with relevant open source communities to stay informed about significant updates, patches and best practices for using and updating their FOSS component.

EXAMPLES OF EVIDENCE

- Contract clauses that include, in addition to the elements referred to in point 5.1.4 of the Annex to the regulation, one or more of the above lists with additional elements.
- Evidence of awareness trainings.
- Records from crisis management tests (Annex to the regulation, point 4.3.4), if available or written confirmations by the supplier or provider after crisis management tests, which demonstrate the participation of relevant personnel of suppliers and service providers.
- For FOSS (indicative, non-exhaustive list):
  - results from risk assessments of the FOSS,
  - dependency monitoring tools,
  - documentation.

5.2 DIRECTORY OF SUPPLIERS AND SERVICE PROVIDERS

The relevant entities shall maintain and keep up to date a registry of their direct suppliers and service providers, including:

(a) contact points for each direct supplier and service provider;

(b) a list of ICT products, ICT services and ICT processes provided by the direct supplier or service provider to the relevant entities.

GUIDANCE

- Keep the registry up to date to ensure all information is current and accurate, that is, add, update and remove suppliers and service provider from the registry in the event of changes.

([47]) Suppliers do not necessarily need to perform security audits (and the resulting remediation efforts) themselves, but they can fund existing initiatives that perform open source security audits at scale (e.g. Sovereign Tech Agency, Alpha-Omega and the Open Source Technology Improvement Fund) or upstream (e.g. by funding a maintainer or by establishing contractual relationships with relevant Open Source Software Stewards to do that work). Additionally, suppliers and service providers should make any code reviews reusable for others to align with manufacturer obligations under Article 13(6) of the Cyber Resilience Act.
The term ‘upstream’ and ‘downstream’ denotes whether a component is being depended on (is upstream of) or is a dependent of (is downstream of) a component.

- Conduct reviews of the registry, at least annually or when significant changes occur to ensure all information is current and accurate.

EXAMPLES OF EVIDENCE

- Registry of direct suppliers and service providers.
- Evidence of registry updates following direct supplier and service provider changes.
- Review plans or schedules.

TIPS

GUIDANCE

- In addition to the elements referred to in point 5.2 of the Annex to the regulation consider the start and end dates of the contract and the region of each direct supplier and service provider.
- Classify direct suppliers and service providers. The classification may include one or more characteristics (indicative, non-exhaustive list):
  - sensitivity of assets purchased,
  - volume of assets purchased,
  - availability requirements,
  - applicable regulations,
  - inherent risk and mitigated risk.
- Update and review classifications annually or when significant changes occur. Examples of categories may be:
  - critical – those with a significant impact on the entity’s operations;
  - strategic – high-value partners who contribute to information assets, for example cloud providers, data analytic providers, software developers and telecommunication providers;
  - routine – those with minimal impact on the entity.

EXAMPLES OF EVIDENCE

- List of relevant contracts or SLAs that are in line with the documented supply chain policy.
- Evidence that the entity has categorised its direct suppliers and service providers based on criteria.
- A clear description of how direct suppliers and service providers are grouped and managed based on their importance and risk level.
- Evidence that the entity assesses risks associated with each direct supplier and service provider category, and that it tailors measures accordingly. For instance, ‘critical’ direct suppliers and service providers receive more attention and customised policies.

SECURITY IN NETWORK AND INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

6. SECURITY IN NETWORK AND INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

6.1 SECURITY IN ACQUISITION OF ICT SERVICES OR ICT PRODUCTS

6.1.1. For the purpose of Article 21(2), point (e) of Directive (EU) 2022/2555, the relevant entities shall set and implement processes to manage risks stemming from the acquisition of ICT services or ICT products for components that are critical for the relevant entities' security of network and information systems, based on the risk assessment carried out pursuant to point 2.1, from suppliers or service providers throughout their life cycle.

GUIDANCE

- Integrate cybersecurity as a permanent component of the purchase process by dedicating a specific section to addressing it. This includes any acquisition processes for selecting FOSS ([48]).
- Document the process for secure acquisition of ICT services, systems or products and describe relevant procedures that support the process.
- Take into account industry-recognised standards when developing the process ([49]).

EXAMPLES OF EVIDENCE

- Tender templates for the acquisition of ICT services, systems or products which address cybersecurity.
- Documented process which is based on relevant standards and good practices.

6.1.2. For the purpose of point 6.1.1., the processes referred to in point 6.1.1. shall include:
(a) security requirements to apply to the ICT services or ICT products to be acquired;
(b) requirements regarding security updates throughout the entire lifetime of the ICT services or ICT products or replacement after the end of the support period;
(c) information describing the hardware and software components used in the ICT services or ICT products;
(d) information describing the implemented cybersecurity functions of the ICT services or ICT products and the configuration required for their secure operation;
(e) assurance that the ICT services or ICT products comply with the security requirements according to point (a);
(f) methods for validating that the delivered ICT services or ICT products are compliant to the stated security requirements, as well as documentation of the results of the validation.

([48]) See section 5.1 (Tips), for additional guidance on the use of free and open source software supply chain.
([49]) In addition, to those mentioned in the mapping table at the end of this section, consider the following:
- https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and services;
- Department of the Environment, Climate and Communications, 'Guidelines on cyber security specifications (ICT procurement for public service bodies)', https://www.ncsc.gov.ie/pdfs/Guidelines_on_Cyber_Security_Specifications.pdf.

GUIDANCE

- The security requirements must include at least the means to detect, monitor and protect against unauthorized changes of software and information.
- Ensure that support contracts cover the system life cycle and obsolescence management requirements, including the date until which the system must be supported and include continuous alerting.
- Favour vendors that provide clear end-of-life information and that plan to provide separate critical security fixes.
- Make sure that tenders request that suppliers or service providers provide tested solutions for security issues in legacy or new technologies free of charge and as soon as a relevant security issue becomes known.
- Consider also the following information describing implemented cybersecurity functions such as (indicative, non-exhaustive list):
    - the potential risks that could arise from acquiring the specific ICT service, system or product. This might involve penetration testing to identify threats, vulnerabilities and the potential impact on the entity's operations;
    - potential security tools that already need to be in place, for example a firewall, an intrusion detection system, a SIEM or a EDR/XDR;
    - a specific security mechanism that might need to be in place, such as a specific encryption algorithm or a particular access control mechanism (e.g. MFA);
    - cybersecurity standards for the ICT service, system or product that the entity needs to comply with;
    - where appropriate, the required assurance level of the ICT product, system or service and the existence of a relevant certificate following the European Cybersecurity Scheme for ICT products based on Common Criteria (EUCC).
- Consider evaluating the security of an ICT service, system or product before acquisition ([50]).

EXAMPLES OF EVIDENCE

- Past or ongoing tenders for acquiring ICT services, systems or products, that address cybersecurity by referring, as a minimum, to the elements outlined in point 6.1.2 of the Annex to the regulation.
- Comparison between selected contracts and the associated tenders to check whether the supply chain policy and particularly the elements referred to in points 5.1.4 and 5.1.5 of the Annex to the regulation, are taken into consideration.
- Records from security tests before acquiring an ICT system or product.
- Certificates, test reports or other supporting information for the ICT products or systems from suitably accredited conformity assessment bodies.

([50]) Criteria for open source components should take into account the voluntary nature of open source projects. Acquirers of such components must constructively engage with project maintainers in addressing Identified security requirements and introducing mitigations and/or improvements. These improvements should be shared with the open source project under their license and terms.

6.1.3. The relevant entities shall review and, where appropriate, update the processes at planned intervals and when significant incidents occur.

GUIDANCE

- Review the processes for secure acquisition of ICT services, systems or products, and the procedures based on them, at least annually.
- Review logs or records of all changes made to the processes for secure acquisition of ICT services, systems or products, and the procedures based on them, including details of the changes, approvals and implementation dates.
- Align the tenders and contracts with the entity's supply chain security policy (Annex to the regulation, point 5.1).
- For ICT services, systems or products that are not provided by a supplier (e.g. open source projects), entities should share relevant results from internal assessments with them.

EXAMPLES OF EVIDENCE

- Review plans or schedules for processes for secure acquisition of ICT services, systems or products, and the procedures based on them.
- Minutes from reviews or possible changes made to the processes for ICT services, system or product acquisition, and the procedures based on them, including actions taken to enhance security in future acquisitions.
- Documented results of possible auditing activities, indicating compliance with internal secure acquisition of ICT services, systems or products processes and external regulations.
- Change management records of changes made to the processes for secure acquisition of ICT services, systems or products, and the procedures based on them, including documentation of the review and approval process.
- Incident response records that confirm whether the entity takes into account significant incidents when reviewing and updating the processes and procedures for secure acquisition of ICT services, systems or products.

TIPS

GUIDANCE

- Apply the secure acquisition of ICT systems or product processes and relevant procedures to both software and hardware products, regardless of whether they were developed in-house or acquired.
- Continuously monitor suppliers or service providers with regard to points 5.1.6 and 5.1.7 of the Annex to the regulation so that they are aligned with the supply chain security policy.
- In addition to the elements referred to in point 6.1.2 of the Annex to the regulation, consider the following when formulating tenders with cybersecurity in mind (indicative, non-exhaustive list):
  - ensure continuous alerting, patching and mitigation proposals if vulnerabilities in the system or the product are discovered;
  - clarify the supplier's or service provider's liability in the event of cyber-attacks or incidents relevant to the service, system or product; and
  - consider cybersecurity during project implementation and before handover including (indicative, non-exhaustive list):
    - design reviews;

  - acceptance tests;
  - commissioning tests;
  - site acceptance tests; and
  - documentation.
- Make sure that secure decommissioning service providers involve considerations such as deactivating user and service accounts, terminating data flows and ensuring the secure disposal of the entity's data within supplier or service provider systems.
- Free and open-source software is often obtained free of charge from communities and projects developing, maintaining and distributing software, as opposed to purchased from suppliers or service providers. When using such software without purchase, relevant entities cannot impose obligations for compliance beyond the adherence to the terms of the open source software license. Beyond that, it is good practice to apply the guidance of section 6.1.

EXAMPLES OF EVIDENCE

- Evidence that internal (in-house) projects consider and prioritize security when acquiring ICT services, systems or product processes.
- Evidence that points 5.1.6 and 5.1.7 of the Annex to the regulation are implemented.
- Tenders that contain elements in addition to those referred to in point 6.1.2 of the Annex to the regulation.

6.2 SECURE DEVELOPMENT LIFE CYCLE

6.2.1. Before developing a network and information system, including software, the relevant entities shall lay down rules for the secure development of network and information systems and apply them when developing network and information systems in-house or when outsourcing the development of network and information systems. The rules shall cover all development phases, including specification, design, development, implementation and testing.

GUIDANCE

- Take into account the entity's policies and norms (if available) and industry-recognised standards when developing the rules for the secure development of network and information systems ([51]).

EXAMPLES OF EVIDENCE

- Documented rules for the secure development of network and information systems which align with the entity's policies and norms and are based on relevant standards and good practices.

6.2.2. For the purpose of point 6.2.1., the relevant entities shall:

(a) carry out an analysis of security requirements at the specification and design phases of any development or acquisition project undertaken by the relevant entities or on behalf of those entities;

(b) apply principles for engineering secure systems and secure coding principles to any information system development activities such as promoting cybersecurity-by-design, zero-trust architectures;

(c) lay down security requirements regarding development environments;

[51] In addition, to those mentioned in the mapping table at the end of this section, consider the following:
- 'OWASP ASVS (Application Security Verification Standard)', https://owasp.org/www-project-application-security-verification-standard/ , as updated from time to time.
- ISO/IEC 27034 family, Information technology - Security techniques - Application security.
- NIST SP 800-53, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final, as updated from time to time.

(d) establish and implement security testing processes in the development life cycle;

(e) appropriately select, protect and manage security test data;

(f) sanitise and anonymise testing data according to the risk assessment carried out pursuant to point 2.1.

GUIDANCE

- A secure software development life cycle (SSDLC) process should be implemented by all entities. However, smaller entities can use a less demanding process such as implementing secure-by-design practices and security-testing processes.
- Depending on the type of requirement, the rules for the secure development of software and systems should include appropriate software testing methods (e.g. black-box, ad-hoc testing, static versus dynamic application security testing).
- Test security by design at various stages of the secure development of the SSDLC prior to go-live, utilising independent tools and a self-service testing platform throughout the SSDLC.
- When real production data - or derived variations of it - is used for testing, ensure that such data is properly sanitised or anonymised. An indicative, non-exhaustive list of techniques:
    - masking or pseudonymization on fields like names, emails, IDs;
    - deletion or redaction of identifiers (e.g. personal IDs, birth dates, ZIP codes); and
    - non-irreversible or one-way anonymisation.
- When using Free and Open Source Software components, entities should take into account the voluntary nature of open source projects (see guidance of section 5.1). Where possible, entities should assist the open source projects that they depend on in adopting secure systems and secure coding principles (such as introducing SSDLC processes suited to the project's way of working).

EXAMPLES OF EVIDENCE

- Evidence that secure development rules have been adopted (indicative, non-exhaustive list):
    - documentation for each phase of the life cycle,
    - process and workflow diagrams,
    - audit and testing reports,
    - version control,
    - change management logs,
    - code reviews, and
    - project management tools.
- Evidence of the test results from secure development environments, including that measures for protecting test data are maintained.
- Evidence of the software-testing methods chosen for a particular test scenario and an explanation of the choice.
- Test results of each phase of the SSDLC maintained and up to date.
- Test results maintained and, where appropriate, approved by management bodies.
- Evidence that a software-testing method is chosen at each stage of the software development life cycle.

6.2.3 For outsourced development of network and information systems, the relevant entities shall also apply the policies and procedures referred to in points 5 and 6.1.

GUIDANCE

- Align the secure development rules with the security testing policy (Annex to the regulation, point 6.5) and procedures and with the secure acquisition of ICT services, systems or product processes (Annex to the regulation, point 6.1).
- Communicate the internal development rules with the relevant personnel from outsourced development.
- Hold regular cross-organisational unit meetings during all phases of the development life cycle.

EXAMPLES OF EVIDENCE

- Comparison of the secure development rules with the security-testing policy and with the secure acquisition of ICT services, systems or product processes, checking whether the security requirements are set consistently in all these documents.
- Evidence of communicating the internal development rules with relevant personnel from outsourced development.
- Records or minutes from cross organisational unit meetings where the development of a network and information system, including software, was discussed.

6.2.4 The relevant entities shall review and, where necessary, update their secure development rules at planned intervals.

GUIDANCE

- Review the rules for the secure development of network and information systems at least once every two years.

EXAMPLES OF EVIDENCE

- Documentation that outlines the schedule and frequency for reviewing secure development rules.
- Documented evidence of the process for reviewing the patch development process and secure-by design software configurations.
- Meeting minutes, review findings and actions taken to improve the development rules.
- Version history or change log of secure development procedures showing updates made as a result of reviews.
  - Specific sections in the documents highlighting what changes were made and the rationale behind them.
- Reports from internal and external audits that evaluate the process for reviewing secure development rules.
- Documentation of change requests related to secure development rules, including those arising from review findings.
- Logs or records tracking the implementation of changes to ensure they are applied throughout the development process.

TIPS

GUIDANCE

- Consider threat modelling as part of the security requirements analysis.
- Keep separate environments for development purposes, testing purposes and production.
- Ensure the use of results of application assessments to regularly enhance developer training and the SSDLC process.
- Defined methods and tooling for performing analysis and tracking of usage of third party libraries should be in place.
- Consider integrating root cause analysis results into SSDLC process changes, if any.
- In addition to the regular reviews, the entity should review and, where necessary, update its secure development rules when there are significant changes to technology, operations or risks or in the event of significant incidents.

EXAMPLES OF EVIDENCE

- Evidence of the use of threat modelling (indicative, non-exhaustive list):
  - documentation of the process used for example STRIDE or DREAD,
  - data flow diagrams, and
  - meeting minutes.
- Evidence of separate environments for development, testing and production, for example different network segments, servers, databases, existence of accounts used for this purpose and change management records.
- Relevant personnel aware of the secure development rules.
- Meeting minutes, logs, reports, etc. showing that the secure development rules were reviewed and possibly changed following significant changes to technology, operations or risks or in the event of significant incidents.

6.3 CONFIGURATION MANAGEMENT

6.3.1. The relevant entities shall take the appropriate measures to establish, document, implement and monitor configurations, including security configurations of hardware, software, services and networks.

GUIDANCE

- Establish documented processes based on best practices and information security standards ([52]).
- Maintain and document detailed configuration settings for the following operating procedures (indicative, non-exhaustive list):
  - processing and handling of information,
  - backup,
  - scheduling requirements, including interdependencies with other systems,
  - handling errors or other exceptional conditions,
  - system restart and recovery procedures,

([52]) In addition to the standards in the mapping table, consider the following:
- ISO/IEC 20000, which is the international standard for IT service management and consists of 17 parts;
- Information Technology Infrastructure Library;
- Institute of Electrical and Electronics Engineers 828, Standard for configuration management in systems and software engineering.

  - cryptographic mechanisms and settings, and
  - audit trail and system log information.
- Consider the following security-related parameters for the configuration settings (indicative, non-exhaustive list):
  - registry settings,
  - account, file and directory permission settings, and
  - settings for functions, ports, protocols, services and remote connections.
- Employ automated mechanisms to centrally manage, apply and verify configuration settings for software and hardware, including mobile devices and the entity's connected vehicles.
  - Where appropriate, implement a configuration management database to catalogue and classify all configuration items (CIs), including their security attributes (e.g. patch level, firewall rules and encryption status)
- Ensure that all network, software and system configurations adhere to established security and operational standards for functions, ports, protocols and services.
- Monitor and control changes to the configuration settings in accordance with the entity's policy on the security of network and information systems and topic-specific policies and procedures.
- Identify software not authorised to run on the information systems.
- Where appropriate, regularly review and update software configurations.
- Where appropriate, identify software programs authorised to run on the information system.
- Employ a deny-all, permit-by-exception policy to allow authorised software to run.
- Set up procedures for network service usage to restrict access to necessary services or applications only.
- Manage a secure baseline configuration for development and test environments separately from the operational baseline configuration, where appropriate.
- Identify, document and approve any deviations from established configuration settings based on defined exceptions on operational requirements.

EXAMPLES OF EVIDENCE

- System configuration process, based on good practices and standards, in place and maintained.
- System configuration tables containing configurations of hardware, software, services and networks.
- Documented secure baseline configuration containing at least (indicative, non-exhaustive list):
  - essential capabilities of operation;
  - restricted use of functions;
  - security by default;
  - ports, protocols and/or services allowed.
- Documented and approved exceptions to the configuration baseline containing the alternative measures in place to ensure the confidentiality, availability and integrity of the CI.
- Documented secure baseline configuration for development and test environments.

6.3.2. For the purpose of point 6.3.1., the relevant entities shall:

(a) lay down and ensure security in configurations for their hardware, software, services and networks;

(b) lay down and implement processes and tools to enforce the laid down secure configurations for hardware, software, services and networks, for newly installed systems as well as for systems in operation over their lifetime.

GUIDANCE

- Consider hardening guides/best practices and general cybersecurity principles (e.g. least functionality and least privilege) as a basis for deriving the defined security configurations.
- Establish, document and maintain configuration settings respecting the access control policy.
- Where applicable, test the configuration before implementation.
- Employ security safeguards to detect and respond to unauthorised changes to defined configuration settings.
- Establish a configuration management plan containing:
  - roles, responsibilities and configuration management processes and procedures;
  - a process for identifying CIs throughout the system development life cycle; and
  - a process for managing the configuration of the CIs throughout their life cycle.
- Protect the configuration management plan from unauthorised disclosure and modification.
- Implement enhanced controls, including regular vulnerability scanning, strict configuration hardening, isolation where feasible and continuous monitoring to compensate for products which lack official updates after the end of supplier support.

EXAMPLES OF EVIDENCE

- Configuration management plan.
- Comparison of the configuration plan with the access control lists.
- Mechanisms, for example logical and physical access controls, encryption and audit logs in place.
- Documented and approved exceptions to the configuration baseline containing the alternative measures in place to ensure the confidentiality, availability and integrity of the CI.

6.3.3. The relevant entities shall review and, where appropriate, update configurations at planned intervals or when significant incidents or significant changes to operations or risks occur.

GUIDANCE

- Review and, where appropriate update ([53]) configurations at least monthly to ensure that patches have been applied, that the backup has been executed according to the plan and that monitoring is in place to identify and alert to fatal server/device/disk errors without delay.
- Regularly produce, keep and review change logs regarding the security configuration of information systems.
- Review and update the configurations after major changes (e.g. software updates) and past incidents.
- Where feasible, obtain baseline configuration files for key systems and devices to compare against current configurations.

EXAMPLES OF EVIDENCE

- Up-to-date configuration management plan, review comments and/or change logs.

([53]) The decision about the update should be based on the actual technical capabilities and specific needs of the entity, taking into account the results of a risk assessment before implementing the update.

- Documented results of the review activities.
- Configuration snapshots taken before and after changes or at regular intervals to verify that reviews are conducted and documented.
- Audit logs from systems and devices that track configuration changes and reviews.
- Alerts from monitoring systems that notify administrators of unexpected configurations or changes or deviations from the baseline in critical systems.
- Audit trails and compliance records from internal and external audits.
- Minutes from team meetings where configuration reviews and changes are discussed and documented.
- Records of notifications or reminders sent to relevant employees about upcoming configuration reviews.
- Records from the configuration management tools to ensure they are kept up to date with accurate configuration information.
- Incident response records that confirm whether the entity takes into account incidents related the configurations.

6.4 CHANGE MANAGEMENT, REPAIRS AND MAINTENANCE

6.4.1. The relevant entities shall apply change management procedures to control changes of network and information systems. Where applicable, the procedures shall be consistent with the relevant entities' general policies concerning change management.

GUIDANCE

- Take into account industry-recognised and national standards when developing the change management procedures ([54]).
- Consider the following elements for the procedures (indicative, non-exhaustive list):
  - request for change,
  - risk assessment,
  - criteria for categorisation and prioritisation of changes:
    - associated requirements for the type and scope of the tests to be carried out and
    - the approvals to be obtained;
  - requirements for performing rollbacks; and
  - documentation of the changes and approval of changes.
- The change management procedures may allow different workflows depending on the criticality of the system, the scope of the change and the urgency (e.g. put in place an 'emergency intervention workflow').
- For each change, record the steps of the procedure followed.
- Review and approve changes following the change management procedures, prior to implementing them.
- Implement and test change management procedures to make sure that changes to networks and information systems are always done in a predefined way.
- Where appropriate, establish a change advisory board (CAB) to oversee and approve changes. The CAB should evaluate change requests based on risk, impact, resource requirements and alignment with business objectives.

([54]) In addition to those mentioned in the mapping table at the end of this section, consider the following:
- ISO 21500:2021, Project, programme and portfolio management - Context and concepts;
- ISO 21502:2020, Project, programme and portfolio management - Guidance on project management.

EXAMPLES OF EVIDENCE

- Documented change management procedures for network and information systems that are based on standards or good practices.
- For each relevant change, a record describing the steps and the result of the change.
- A system maintenance procedure that addresses:
    - purpose;
    - scope;
    - roles;
    - responsibilities;
    - management commitment, if applicable;
    - coordination among different organisational units; and
    - compliance.
- Logs that record the dates and outcomes of the periodic reviews of the change, repair and maintenance procedures.

6.4.2. The procedures referred to in point 6.4.1. shall be applied for releases, modifications and emergency changes of any software and hardware in operation and changes to the configuration. The procedures shall ensure that those changes are documented and, based on the risk assessment carried out pursuant to point 2.1, tested and assessed in view of the potential impact before being implemented.

GUIDANCE

- Consider a mandatory integrity check before installing and deploying new software.
- Ensure, where appropriate, that changes are done in an authenticated, authorised and non-repudiating manner.
- Test and validate changes before they are implemented in operational systems, where applicable. Where appropriate, a security impact analysis may be performed in a separate test environment before implementation in an operational environment.
- Take all necessary precautions before making changes (back up images, for instance).
- Schedule, perform, document and review records of maintenance and repairs on system components in accordance with the supplier’s specifications and/or the entity’s requirements.
- Ensure that changes are only allowed with approved tools and that their execution is documented.
- Restrict the use of maintenance tools to authorised personnel only.

EXAMPLES OF EVIDENCE

- Logs and records of past (new) software installations.
- Evidence that MFA is in place for activating change, repair and maintenance procedures, where applicable.
- Test plans and results that demonstrate the implementation and effectiveness of the change, repair and maintenance procedures.
- If the entity utilises change management tools, evidence that these tools enforce the use of approved resources only and mandate documentation for each change.
- Access control lists (ACLs) to verify that access to the tools is in line with the access control policy.

6.4.3. In the event that the regular change management procedures could not be followed due to an emergency, the relevant entities shall document the result of the change and the explanation for why the procedures could not be followed.

GUIDANCE

- Where appropriate, integrate the pullback scenario ([55]) into the change management procedures.
- Assess the risks from legacy systems and upgrade existing legacy systems to include security mitigating measures in case appropriate security cannot be achieved.
- Make sure that regular change control procedures that could not be followed due to an emergency change are applied immediately after the emergency change.

EXAMPLES OF EVIDENCE

- Documentation with specific pullback plans.
- Logs and records of past change requests with details of (indicative, non-exhaustive list):
    - the change,
    - reason for emergency,
    - approval,
    - reason for delay,
    - follow up actions and
    - how to revert the system to a previous stage if the change fails.
- Logs and records from past legacy system upgrade that contain risk assessments and the reasoning for the change.

6.4.4. The relevant entities shall review and, where appropriate, update the procedures at planned intervals and when significant incidents or significant changes to operations or risks.

GUIDANCE

- Review the change management procedures at least once every two years.
- Make sure that the management procedures cover planned and unplanned changes and the development phase, when applicable.
- Ensure that the process is not bypassed.

EXAMPLES OF EVIDENCE

- Review plans or schedules.
- Up to date change management procedures, review comments and/or change logs.
- Evidence of approval and monitoring of maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.
- Logs of all changes made to the procedures, including details, approvals and implementation dates.
- Audit trails and compliance records from internal and external audits.
- Logs of significant incidents to confirm whether they include documentation of reviews and updates to the change, repair and maintenance procedures.

([55]) Also known as a roll-back or backout plan, it refers to a set of pre-planned actions or procedures designed to revert a system or a service to a previous, stable, state in case the change does not work as expected.

- Reports from post-incident reviews that document any necessary adjustments to the procedures following significant incidents.
- Records showing how changes and updates to the procedures were implemented and reviewed.

TIPS

GUIDANCE

- Perform and log: (a) changes to, (b) maintenance of and (c) repairs to network and information systems, with approved and controlled tools.
- Put change management procedures in place according to licensing agreements.
- Upon changes to assets, update the asset inventory (Annex to the regulation, point 12.4) and documentation.
- Upon changes to risk management measures, update the risk treatment plan (Annex to the regulation, point 2.1.1).
- Inform the customer of significant changes to network and information systems that affect the services offered. This information only needs to be provided if it is beneficial for customers.
- Ensure availability of the required maintenance skills, resources and spare parts, including external support.
- Prevent the unauthorised removal of maintenance equipment containing information related to the entity by (indicative, non-exhaustive list):
    - verifying that no information related to the entity is contained in the equipment;
    - sanitising or destroying the equipment;
    - retaining the equipment within the facility; or
    - obtaining an exemption from authorised personnel or roles explicitly authorising removal of the equipment from the facility.
- Provide remote access via out-of-band (OOB) connection in the event that the standard connection does not work.
- Regularly test OOB connections to ensure they function as expected during an outage.
- If an incident, in the sense of Article 23 of the NIS2 Directive, involves subsequent actions that entail system changes, then notify the competent authorities of these changes in accordance with the national reporting procedure.

EXAMPLES OF EVIDENCE

- Evidence that MFA is in place for remote change, repair and maintenance procedures.
- Logs and records that prove the use of approved tools.
- Evidence that the procedures mention the licencing agreement.
- Up-to-date asset inventory.
- Up-to-date risk-treatment plan.
- Documentation of a customer update on significant changes.
- Evidence of previous training on change management and system maintenance.
- Evidence of sanitisation procedures.
- Evidence that the entity maintains a spare parts for key components of its network and information system.
- Notifications to defined personnel or roles of the date and time of planned maintenance.
- Network architecture diagram that proves the existence of OOB connections.

6.5 SECURITY TESTING

6.5.1. The relevant entities shall establish, implement and apply a policy and procedures for security testing.

GUIDANCE

- Take into account industry-recognised standards when developing the testing policy ([56]).
- Establish and maintain a testing programme appropriate to the entity's size, complexity and maturity ([57]).

EXAMPLES OF EVIDENCE

- Documented security testing and procedures based on relevant standards and good practices.
- Guidelines and standards that the entity adheres to for conducting security tests.

6.5.2. The relevant entities shall:

(a) establish, based on the risk assessment carried out pursuant to point 2.1, the need, scope, frequency and type of security tests;

(b) carry out security tests according to a documented test methodology, covering the components identified as relevant for secure operation in a risk analysis;

(c) document the type, scope, time and results of the tests, including assessment of criticality and mitigating actions for each finding;

(d) apply mitigating actions in case of critical findings.

GUIDANCE

- Make sure that network and information systems undergo continuous testing, particularly in environments utilizing continuous integration / continuous deployment practices. Regular testing should be conducted at set-up, after significant upgrades or modifications and following maintenance, to maintain robust security and performance.
- Consider a range of security tests (e.g. vulnerability assessments, penetration testing, code review, ethical hacking, bug bounty programmes, cyber attack simulations, red teaming, protocol conformance testing or cyber response exercises) and select the most appropriate one (or more) to test the specific procedure, service or tool over time.
- Entity-wide scoped tests should be carried out at planned intervals or when significant incidents or changes occur.
- Conduct internal and/or external audits throughout the entity's networks, systems and processes in an ad-hoc manner.
- Record evidence while testing. The need, scope, frequency, type and results are to be documented in a manner that is comprehensible to an expert third party.
- Use criteria to assess the results of the tests similar to the criteria for performing cybersecurity risk assessments (guidance on point 2.1.2 of the Annex to the regulation).
- Assess, follow up and remediate high-criticality findings with respect to the confidentiality, integrity, authenticity or availability of the service provided.

([56]) In addition to the standards in the mapping table, consider the following:
- ISO/IEC 27034 series of standards on application security.
- OWASP Web Security Testing Guide, https://owasp.org/www-project-web-security-testing-guide/.
- Open Source Security Testing Methodology Manual (OSSTMM), https://www.isecom.org/OSSTMM.3.pdf.

([57]) CyberFundamentals, ID.RA-1, Centre for Cyber Security Belgium, https://atwork.safeonweb.be/sites/default/files/2024-12/cyfun_basic_v2023-03-01_e_update_2024.pdf.

- Document the assessment of criticality and mitigating actions for each finding. Ensure that risk assessment results and risk treatment plans are updated accordingly (Annex to the regulation, point 2.1).
- When testing reveals an underlying security issue in a free and open source component, these findings must be shared with the relevant open source project. If a patch is developed to address the issue, the relevant code should also be shared with the relevant open source project, in a manner suitable for integration.
- Where appropriate, any automated security tests written by entities for open source components that they use, should be shared with the relevant open source projects.

EXAMPLES OF EVIDENCE

- Documented security testing policy and procedures that include the elements referred to in point 5.2 (a) of the Annex to the regulation.
- Documentation defining the roles and responsibilities of personnel involved in security testing.
- Plans or schedules for upcoming or completed regular or ad hoc tests.
- List of reports from past security tests This should cover various types of testing (e.g. vulnerability assessments, penetration testing and code reviews).
- Internal or external audit reports.

6.5.3. The relevant entities shall review and, where appropriate, update their security testing policies at planned intervals.

GUIDANCE

- Review the security testing policy and procedures at least once every two years.

EXAMPLES OF EVIDENCE

- Updated security-testing policy and procedures, review comments, and/or change logs.
- Security-testing policy and procedures, including when tests must be carried out, test plans, test cases and test report templates.

TIPS

GUIDANCE

- For systems with external integrations (e.g. cloud services) beyond the organization’s control, ensure that all external application programming interface endpoints are thoroughly tested.
- Determine the auditable security events that are adequate for supporting investigations of security incidents.
- Implement tools for automated testing, such as code analysis tools or vulnerability scanners.
- Ensure the policy is approved by, communicated to and acknowledged by relevant personnel and third parties.
- Ensure that the development and testing environment(s) is/are separate from the production environment.
- Review the security-testing policy and procedures when significant incidents or major changes to the network and information system occur.

EXAMPLES OF EVIDENCE

- In addition to the elements referred to in point 6.5.2 (c) of the Annex to the regulation, documented policy that includes at least (indicative, non-exhaustive list):
  - approved parties (internal or third);
  - confidentiality levels for assessment; and

  - test results and the objectives of security assessments and tests.
- Relevant staff aware of the security-testing procedures and tools.
- Documented audit requirements.
- A list of tools used for security testing, including their purpose and how they are maintained and updated.
- Valid licences for commercial testing tools or subscriptions to security services.
- Review showing that the security tools are in use and configured to perform the actions intended.
- Records showing updates to the security policy and procedures based on lessons learnt and new threats.

6.6 SECURITY PATCH MANAGEMENT

6.6.1. The relevant entities shall specify and apply procedures, coherent with the change management procedures referred to in point 6.4.1. as well as with vulnerability management, risk management and other relevant management procedures, for ensuring that:

(a) security patches are applied within a reasonable time after they become available;

(b) security patches are tested before being applied in production systems;

(c) security patches come from trusted sources and are checked for integrity;

(d) additional measures are implemented and residual risks are accepted in cases where a patch is not available or not applied pursuant to point 6.6.2.

GUIDANCE

- Take into account well known standards when developing the security patch management procedures ([58]).
- Actions may vary, depending on the network and information system (e.g. mandatory patching for all exposed systems or internet-connected devices such as firewalls or routers, and limited patching only in specific circumstances, for instance in isolated or legacy systems where regular patching may not be feasible or available).
- Establish a process, in combination with the asset inventory, for being informed when a new security patch is published and schedule patch roll-outs accordingly.
- Patching should be a standard activity in normal maintenance and outage planning of services. Nonetheless, some failures may require immediate patching depending on their criticality.
- Prioritise and apply patches based on risk. Evaluate the severity of the vulnerability, exposure of the affected system and likelihood of exploitation.
- Deploy vulnerability management technologies to identify unpatched and misconfigured software.
- Define your relevant security information sources considering your assets and continuously monitor them for patch announcements, patch and non-patch remediation, and general threats.
- Verify the patch sources through (indicative, non-exhaustive list):
  - digital certificates to verify the vendor;
  - digital signatures of the patches
  - change logs provided by the vendor; and
  - feedback from the community concerning the reliability of the vendor.
- Consider a strategy for applying patches after approval or testing following the change management procedure (indicative, non exhaustive list):

([58]) NIST SP 800-40 Rev. 4, 'Guide to enterprise patch management planning: preventive maintenance for technology', https://csrc.nist.gov/pubs/sp/800/40/r4/final.

  - Blue/green allows the patches to be applied first in an isolated environment identical to the production environment, and then in the production environment. This ensures zero downtime and an immediate rollback option.
  - Rolling ([59]) deployment allows gradual updates of parts of the production environment, one set of servers or instances at a time, rather than deploying a patch all at once. It is ideal for large and distributed environments.
  - Feature toggles allow new features or patches to be deployed to production but keep them disabled until they are ready to be used. They are suitable for control over new features or patches when they are turned on, making it easy to test and release.
  - Shadow deployment allows new code or patches to be deployed directly to production but it shadows live traffic by mirroring user requests to both the current and new systems to observe how the new version behaves without affecting the user experience. It is ideal for testing new features in production without affecting users.
  - Hotfix deployments are used for critical patches that need to be applied immediately to address severe issues.
- Where appropriate and to reduce risks related to significant updates in important dependencies, consider performing a trial using *release candidates* ([60]) of these components, to get an early indication of incompatibilities or breaking changes, so they may be remedied. If any of these components are open source software, offer feedback about any issues found during this trial.

EXAMPLES OF EVIDENCE

- Detailed procedures and guidelines for how patches are identified, evaluated, tested, deployed and verified.
- Logs or records showing the history of patch deployments across various systems. These may include (indicative, non-exhaustive list):
  - timestamps;
  - responsible personnel; and
  - affected systems.
- Evidence that the asset inventory (Annex to the regulation, point 12.4) is updated after a new security patch is announced, if possible accompanied by the time plan for applying it.
- Evidence of testing patches before deployment in a controlled environment. This should include results of testing and any issues encountered and resolved.
- Documentation of test plans and results for patches before deployment to production environments.
- Documentation of change requests for deploying patches, including approvals and impact assessments.
- Detailed audit trails showing the steps taken from patch identification to deployment.
- Checks for the latest patches.
- Approved documented actions for applying patches.
- Records of changes logged, reviewed and approved.
- Evidence of vendor verification mechanisms for example digital certificates and digital signatures.
- Reports from internal and external audits evaluating the effectiveness of the patch management processes.

([59]) 'Canary deployment' is an example of this and refers to a gradual rollout strategy for software updates or patches. To minimise the risk of the patch introducing new problems, the entity might apply the patch to a small number (e.g. 5%) of servers or systems and then gradually apply it to the entire system. It is ideal for rolling out changes slowly and monitoring for problems without affecting many users.
([60]) A release candidate is a 'pre-publication' or 'trial publication' of a software component, usually done in preparation before the publication of a software update with significant changes.

6.6.2. By way of derogation from point 6.6.1.(a), the relevant entities may choose not to apply security patches when the disadvantages of applying the security patches outweigh the cybersecurity benefits. The relevant entities shall duly document and substantiate the reasons for any such decision.

GUIDANCE

- Make an effort, proportionate to the entity's size and importance, to ensure that security patches do not introduce additional vulnerabilities or instabilities. Examples of information supporting such a decision may include (indicative, non-exhaustive list):
    - vendor documentation on the patch:
        - what specific vulnerabilities or bugs are addressed,
        - whether the patch fixes a security issue, improves performance, adds features or resolves stability concerns,
        - system requirements or any specific configurations required or changes to system settings,
        - installation instructions on How to apply the patch and whether it requires a restart or additional configuration;
    - severity rating - patches that address critical vulnerabilities are more likely to apply; and
    - security blogs, forums and mailing lists for any known issues or incompatibilities introduced by the patch.
- If patching is not feasible, consider alternative measures such as strict configuration hardening, intrusion detection systems, regular vulnerability scanning, network segmentation or isolation where feasible, access control and monitoring.

EXAMPLES OF EVIDENCE

- Evidence of patch prioritisation for example emphasis is placed on patches assessed as critical.
- Evidence that residual risks resulting from non-patching are listed and mitigated.
- Incident reports related to unpatched vulnerabilities to check the effectiveness of the mitigation measures during the entity's response.
- Logs of changes made to systems, including patches applied, rollback procedures and any issues encountered.
- Documented decisions no to patch accompanied by relevant alternative measures.
- Up-to-date risk-treatment plan.

TIPS

GUIDANCE

- Patch management procedures should indicate scope, roles and responsibilities.
- Perform operating system and application updates on enterprise assets through automated patch management.
- Use appropriate patch management tools to fulfil the elements referred to in point 6.6.1 of the Annex to the regulation.
- Since patches can sometimes cause issues, it is recommended to back up the system before applying them.
- Have a rollback plan to ensure that the system reverts to a safe previous state if patching does not work or fixing the problem is not feasible.

- Remove unsupported hardware and software from the network in a reasonable and accepted time in line with the entity's risk assessment.
- Include patch and update requirements in the supply chain policy (Annex to the regulation, point 5.1) and in the contracts, bid evaluation and selection criteria for new ICT services, systems or products (section 6.1), considering the system life span among other aspects.

EXAMPLES OF EVIDENCE

- Documentation of regular meetings where patch management processes are reviewed. This should include agendas, attendance records, actions taken to improve the process and minutes from the meetings.
- Checks of the latest patches for evidence of who performed each step and when and for documentation outlining the roles and responsibilities of staff involved in the patch management process.
- Patch management tools.
- Configuration and logs from these tools demonstrating regular use.
- Rollback plan.
- Contract, bid and documented evaluation and selection criteria for new systems which consider the patch management requirements and the system life span.

6.7 NETWORK SECURITY

6.7.1. The relevant entities shall take the appropriate measures to protect their network and information systems from cyber threats.

GUIDANCE

- Take into account well-known standards when implementing measures for network security ([61]).

EXAMPLES OF EVIDENCE

- Documented network security measures that are based on relevant standards and good practices.

6.7.2. For the purpose of point 6.7.1., the relevant entities shall:

(a) document the architecture of the network in a comprehensible and up to date manner;

(b) determine and apply controls to protect the relevant entities' internal network domains from unauthorised access;

(c) configure controls to prevent accesses and network communication not required for the operation of the relevant entities;

(d) determine and apply controls for remote access to network and information systems, including access by service providers;

(e) not use systems used for administration of the security policy implementation for other purposes;

(f) explicitly forbid or deactivate unneeded connections and services;

(g) where appropriate, exclusively allow access to the relevant entities' network and information systems by devices authorised by those entities;

([61]) In addition to those mentioned in the mapping table at the end of this section, consider the following:
a) NIST Special Publication NIST SP 800-215, Guide to a Secure Enterprise Network Landscape, https://doi.org/10.6028/NIST.SP.800-215, accessed 7 May 2025.
b) ISO/IEC 27033 series of standards on network security.

(h) allow connections of service providers only after an authorisation request and for a set time period, such as the duration of a maintenance operation;

(i) establish communication between distinct systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of their end points and protection of the channel data from modification or disclosure;

(j) adopt an implementation plan for the full transition towards latest generation network layer communication protocols in a secure, appropriate and gradual way and establish measures to accelerate such transition;

(k) adopt an implementation plan for the deployment of internationally agreed and interoperable modern e-mail communications standards to secure e-mail communications to mitigate vulnerabilities linked to e-mail-related threats and establish measures to accelerate such deployment;

(l) apply best practices for the security of the DNS and for Internet routing security and routing hygiene of traffic originating from and destined to the network.

GUIDANCE

- Implement secure-by-design principles by integrating security at every layer of network design including the physical, data link, network, transport and application layers.
- Implement secure configurations for wireless networks.
- Where appropriate, consider zero-trust ([62]) network access.
- Identify the technical measures for the transition to the latest network layer communication protocols (e.g. transition to Internet Protocol version 6).
- Define roles, responsibilities and timelines for the transition to latest-generation network layer communication protocols.
- Approve, log and perform remote maintenance of network and information systems in a manner that prevents unauthorised access.
- Consider the following for email communications (indicative, non-exhaustive list):
    - standards such as Start transport layer security (STARTTLS), DNS-based authentication of named entities (DANE), domain-based message authentication, reporting and& conformance (DMARC), DomainKeys identified mail (DKIM) and sender policy framework ([63]),
    - internal spam/scam/virus filtering and
    - URL rewriting, URL scanning and URL detonation in a sandbox.
- Consider DNS security good practices (indicative, non-exhaustive list):
    - deploying DNS security extensions (DNS SEC) ([64]),

([62]) Zero-trust is a security model that assumes no user, device, application or network is trusted by default — even if it's inside the corporate perimeter. It's particularly relevant to remote access, service provider access, network segmentation and device control. Key components to implement zero trust are (indicative, non-exhaustive list):
- Identity and access management supported by MFA (11.6.1), role based access control (11.1.3) and just in time access;
- Device security supported by a policy which allows only known devices and EDR (6.9.2);
- Network microsegmentation supported by logical segmentation (6.8), Next Generation Firewalls and a policy which prevents lateral movement;
- Zero trust network access (ZTNA) supported by replacement of VPNs by ZTNA platforms, monitoring off all access requests and a policy which grants access to resources based on the combination of identity/device trust/context;
- Application and data protection supported by cloud access security brokers (CASBs), data loss prevention (DLP) and encryption as well as monitoring of user activity; and
- Continuous monitoring supported by a SIEM, user and entity behaviour analytics.

([63]) https://ec.europa.eu/internet-standards/email.html.

([64]) 'Secure Domain Name System (DNS) Deployment Guide', http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf, as updated from time to time;
Olaf Kolkman, 'DNSSEC HOWTO, a tutorial in disguise', https://www.dns-school.org/Documentation/dnssec_howto.pdf, as updated from time to time.

  - deploying protective DNS, wherever technically feasible, to provide additional network-wide security capabilities,
  - encrypting DNS traffic, both internal and external, wherever feasible,
  - deploying dedicated DNS servers to reduce attack surface and
  - following all technical guidance on ensuring that DNS deployments and the DNS protocol are as secure and resilient as possible.
- Consider Border Gateway Protocol (BGP) ([65]) for internet routing.

EXAMPLES OF EVIDENCE

- Up-to-date network diagrams, including OOB connections.
- Firewall(s) configured in accordance with the network traffic rules of the entity's policies.
- Configuration files and rulesets for firewalls and routers, showing how traffic is filtered and managed.
- Secure configurations for wireless networks for example use of WPA3 (encryption), 802.1X with EAP (authentication), firmware updates.
- Configuration files for switches, including virtual local access network (VLAN) settings and ACLs.
- Documentation of ACLs implemented on network devices to control traffic flow.
- Documented correct usage of mobile devices, including the entity's connected vehicles that can store data locally on the vehicle and/or share data externally by means of telematics and other remote accesses (e.g. teleworking and OOB connections).
- Evidence of controls over privileged accounts, including logs and policies.
- A list of all devices used (network components), if any, that cannot receive security patches and are not up to date.
- Access logs to confirm that only authorised personnel make changes and conduct reviews of the network security rules.
- Transition to the latest generation plan for implementing network layer communication protocols.

6.7.3. The relevant entities shall review and, where appropriate, update these measures at planned intervals and when significant incidents or significant changes to operations or risks occur.

GUIDANCE

- Although the frequency of reviews of network security measures depends on the entity's risk assessment as a general rule the entity might (indicative, non-exhaustive list):
  - continuously monitor the networks for real time threats;
  - perform scans for new vulnerabilities weekly;
  - review and possibly update the rules of the firewall and other tools monthly; and
  - thoroughly assess the entire network annually.
- Review logs or records of all changes made to the network security rules, including details of the changes, approvals and implementation dates.
- Ensure that these reviews are conducted regularly and documented comprehensively.

([65]) ENISA, *7 Steps to shore up the Border Gateway Protocol (BGP)*, https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp.

EXAMPLES OF EVIDENCE

- Plans or schedules for upcoming or completed, regular or ad hoc reviews.
- List of reports from past reviews. This should cover various types of reviews.
- Logs from firewalls, routers and other network devices showing access attempts, configuration changes and other relevant activities.
- Reports from SIEM and EDR/XDR systems showing aggregated and analysed security events.
- Virtual private network (VPN) and remote access logs showing remote access, including OOB connections, access attempts, successful connections and any anomalies.
- Evidence of network access control (NAC) or other similar and/or alternative solutions, in place, including logs and configuration settings.
- Logs or records showing the dates and results of regular reviews of the network security rules.
- Logs or records of all changes made to the network security rules.
- Logs or records of firewall and ACL reviews.
- Documentation showing regular reviews of user and administrative access to network devices.
- Audit logs from network security devices (e.g. firewalls, intrusion detection/prevention systems (IDS/IPS)) to ensure that changes and reviews are logged.
- Backup files of network device configurations to ensure that changes and reviews are reflected in the backups.
- Logs of network security incidents to see if they include documentation of rule set reviews following significant incidents.
- Post incident review reports to see if they document reviews and any necessary adjustments to the network security rules.

TIPS

GUIDANCE

- Communicate to personnel the correct usage of mobile devices, including the entity's connected vehicles and other remote accesses.
- Where appropriate, apply solutions capable of collecting, analysing and detecting all anomalies, exfiltrations, intrusions and the most sophisticated threats.

EXAMPLES OF EVIDENCE

- The correct usage of mobile devices and other remote accesses (e.g. teleworking and VPN) has been communicated to personnel.
- Existence of IDS/IPS.

6.8 NETWORK SEGMENTATION

6.8.1. The relevant entities shall segment systems into networks or zones in accordance with the results of the risk assessment referred to in point 2.1. They shall segment their systems and networks from third parties' systems and networks.

GUIDANCE

- Take into account well known standards when segmenting networks ([66]).
- Integrate the segmentation derived from the risk assessment into the network diagram.

EXAMPLES OF EVIDENCE

- Documented network segmentation rules based on relevant standards and good practices.

6.8.2. For that purpose, the relevant entities shall:

(a) consider the functional, logical and physical relationship, including location, between trustworthy systems and services;

(b) grant access to a network or zone based on an assessment of its security requirements;

(c) keep systems that are critical to the relevant entities operation or to safety in secured zones;

(d) deploy a demilitarised zone within their communication networks to ensure secure communication originating from or destined to their networks;

(e) restrict access and communications between and within zones to those necessary for the operation of the relevant entities or for safety;

(f) separate the dedicated network for administration of network and information systems from the relevant entities' operational network;

(g) segregate network administration channels from other network traffic;

(h) separate the production systems for the relevant entities' services from systems used in development and testing, including backups.

GUIDANCE[67, 68]

- Make sure that the segments are in line with the results of the risk assessment (Annex to the regulation, point 2.1).
- Apply a graduated set of measures in different logical network domains to further segregate the network security environments, including:
  - publicly accessible systems;
  - internal networks;
  - OOB connections; and
  - assets with high criticality.

([66]) In addition to those mentioned in the mapping table at the end of this section, consider the following:
- NIST, 'Guide to a Secure Enterprise Network Landscape', NIST SP 800-215, https://csrc.nist.gov/pubs/sp/800/215/final.
- ISO/IEC 27033 series of standards on network security.
- NIST SP 800-215 and 1800-35 propose a zero-trust model, which assumes that no part of the network is trusted.

([67]) Different organisations use different terminology for the term 'operational network', for example 'enterprise network', 'corporate network', 'IT network', 'OT network' and 'administration network'. However, the fundamental concept remains focused on the interconnectedness and functionality of components working together towards common objectives set by the management of the entity.

([68]) The network for administration of a network and information system, often referred to as network administration, involves managing, monitoring and maintaining an entity's network infrastructure to ensure its optimal performance and security.

- Implement subnetworks for publicly accessible system components that are physically and/or logically separate from internal organisational networks.
- Determine the degree of physical separation of system components from physically distinct components:
  - in separate racks in the same room,
  - in separate rooms for the components with high criticality and
  - more significant geographical separation of the components with high criticality.
- Implement separate network addresses (that is,, different subnets) to connect to systems in different security domains.
- Monitor and control communications at the external boundary of the system as well as at key internal boundaries within the system, including segmentation violations.
- Where appropriate, isolate information security tools, mechanisms and support components from other internal information system components, where appropriate ([69]), by implementing physically separate subnetworks with managed interfaces to other components of the system.
- Route all networked, privileged accesses through a dedicated, managed interface for the purposes of access control and auditing.
- Implement a managed interface for each external telecommunication service.

EXAMPLES OF EVIDENCE

- Risk assessments that justify the segmentation decisions.
- Interviews with IT and security staff to understand the rationale behind network segmentation.
- Up-to-date network diagrams showing segmentation into different networks or zones (e.g. DMZ ([70]), internal networks and guest networks).
- Verification that the diagrams align with business functions and risk profiles.
- Documented criteria for creating and maintaining different network zones.
- VLAN configurations on network switches and routers.
- VLANs corresponding to different security zones and business functions.
- Measures (e.g. IDS/IPS and monitoring systems) tailored to each network zone.
- Configurations of network devices (e.g. routers, switches and firewalls) for appropriate segmentation settings.
- Configuration settings that match documented segmentation rules and diagrams.
- ACLs that consider segregation of duties.
- Firewall configurations.

([69]) Technical method for segmentation should be considered, the usage of VLAN, physical separate switches or other methods should be defined. However physically separating subnets is not feasible in entirely software-defined environments (container clusters, cloud environments, etc.).
([70]) A perimeter network, also known as a demilitarised zone (DMZ), is a subnetwork that separates an entity's internal network from untrusted external networks, such as the internet. The primary purpose of a perimeter network is to add an extra layer of security by isolating external-facing services from the internal network.

6.8.3. The relevant entities shall review and, where appropriate, update network segmentation at planned intervals and when significant incidents or significant changes to operations or risks.

GUIDANCE

- Review and, if necessary, update the process for network segmentation rules at least annually.

EXAMPLES OF EVIDENCE

- Reports from recent penetration tests and/or vulnerability scans.
- Plans or schedules for reviewing network segmentation rules.
- Logs or records confirming that the reviews have been conducted in accordance with the schedule.
- Change management documentation for network segmentation changes, in line with risk-assessment results and business needs.
- Incident response documentation to verify that network segmentation rules are reviewed following significant security incidents.
- Post-incident analysis reports that include assessments of segmentation rule effectiveness and any necessary adjustments.
- Internal or external audit logs and reports that cover network segmentation rule reviews.
- Reviews performed periodically and in response to network changes or incidents.
- Minutes from security or IT operations meetings where network segmentation rules are discussed.
- Penetration tests and vulnerability assessments that include evaluations of network segmentation.
- Tests conducted periodically and after major changes or incidents and findings leading to rule reviews.

TIPS

GUIDANCE

- Limit the data traffic between the different segments to the operationally required extent by means of data flow control for example a firewall.
- Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the entity's security architecture such as:
  - gateways;
  - routers;
  - firewalls;
  - network-based malicious code analysis;
  - virtualisation systems; and
  - encrypted tunnels.
- Prevent discovery of specific system components composing a managed interface.
- Monitor exceptions.

EXAMPLES OF EVIDENCE

- Network isolation and implementation of segmented network security zones that limit the impact of a malicious software incident.
- Logging and monitoring active for each zone.
- Alerts for segmentation rule violations.
- Reviews triggered by alerts to segmentation violations.

6.9 PROTECTION AGAINST MALICIOUS AND UNAUTHORISED SOFTWARE

6.9.1. The relevant entities shall protect their network and information systems against malicious and unauthorised software.

6.9.2. For that purpose, the relevant entities shall in particular implement measures that detect or prevent the use of malicious or unauthorised software. The relevant entities shall, where appropriate, ensure that their network and information systems are equipped with detection and response software, which is updated regularly in accordance with the risk assessment carried out pursuant to point 2.1 and the contractual agreements with the providers.

GUIDANCE

- Employ mechanisms for detecting and protecting against malicious and unauthorised software at system entry and exit points and at workstations, servers and mobile computing devices on the network to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, web accesses or removable media or inserted through the exploitation of system vulnerabilities.
- Configure malicious code protection mechanisms to:
  - be active all the time;
  - perform periodic scans of the system regularly and real-time scans of files from external sources as the files are downloaded, opened or executed;
  - generate notifications when suspected malicious and unauthorised software is detected;
  - disinfect and quarantine infected files; and
  - restore system settings and ensure that critical settings cannot be disabled or restricted.
- Apply application whitelisting and monitor unauthorised activities and system behaviour, where appropriate.
- Make sure that the malicious and unauthorised protection mechanisms are centrally managed, where appropriate.
- Make sure that there are mechanisms that prevent users from circumventing malicious and unauthorised software protection capabilities.
- Make sure that spam protection mechanisms are employed at system entry points such as workstations, servers or mobile computing devices on the network.
- Update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration rules and the entity's patch management procedures.
- Address issues related to false positives during malicious code detection and eradication and the resulting potential impact on system availability.
- Align rules for monitoring and logging malicious and unauthorised detection and repair software with the entity's monitoring and logging tools and procedures (Annex to the regulation, point 3.2) and with the entity's access control (Annex to the regulation, point 11.1) and asset-handling policy.

EXAMPLES OF EVIDENCE

- Endpoint protection systems (EPS), such as endpoint protection platform (EPP) and endpoint detection and response (EDR), across the network.
- Malware detection system present and up to date.
- Tools for monitoring unauthorised software is in place and up to date.
- Firewall configurations, IDS/IPS and secure web gateways containing malicious and unauthorised software protection measures.
- Use of whitelisting solutions, which restrict the execution of non-approved software and code.

- Rules and configurations related to application whitelisting up to date.
- Documented description of centrally managed tools.
- Records of recent updates of mechanisms for detecting and protecting against malicious/unauthorised software showing that they are regularly patched and updated to protect against known vulnerabilities.
- Records of periodic scans.
- Monitoring and logging of network and information systems, at intervals to identify malicious code and unauthorized code execution.
- Logs of blocked or detected threats.
- Logs recorded and maintained covering:
  - user activities;
  - exceptions; and
  - information security incidents.
- Documented spam protection mechanism.
- Risk assessment to determine the level of logs monitoring required.

TIPS

GUIDANCE

- Consider that the use of malicious and unauthorised detection and repair software alone is not usually adequate or may not be available, so it should be complemented by additional measures such as (indicative, non-exhaustive list):
  - implementing rules and measures that prevent or detect the use of unauthorised software;
  - implementing measures that prevent or detect the use of known or suspected malicious websites;
  - reducing vulnerabilities that can be exploited by malicious software;
  - controlling the running of applications on user workstations or user end devices (including smartphones or tablets);
  - employing web application filters to reduce exposure to malicious content.
- Consider email filters as essential tools for detecting and blocking malicious and unauthorised software. Different types of filter are (indicative, non-exhaustive list):
  - content filter;
  - blocklist filter;
  - antivirus filter;
  - phishing filters; and
  - machine learning filters.

EXAMPLES OF EVIDENCE

- Documented alternative countermeasures such as:
  - securing all physical and logical data interfaces;
  - network isolation and implementation of segmented network security zones that limit the impact of a malicious software incident;
  - comprehensive system-hardening measures to minimise the risk of malicious software incidents.
  - logs confirming that administrative privileges are controlled and monitored.
- Logs from email filters.

6.10 VULNERABILITY HANDLING AND DISCLOSURE

6.10.1. The relevant entities shall obtain information about technical vulnerabilities in their network and information systems, evaluate their exposure to such vulnerabilities and take appropriate measures to manage the vulnerabilities.

GUIDANCE

- Adopt a framework for assessing the severity of vulnerabilities based on models (e.g. CVSS, exploit prediction scoring system (EPSS) or SANS vulnerability assessment framework) and supplemented by environmental and threat metrics as appropriate.

EXAMPLES OF EVIDENCE

- Documentation of a risk-assessment framework used to evaluate the severity, impact and probability of exploitation of identified vulnerabilities (e.g. CVSS scores).

6.10.2. For the purpose of point 6.10.1., the relevant entities shall:

(a) monitor information about vulnerabilities through appropriate channels, such as announcements of CSIRTs, competent authorities or information provided by suppliers or service providers;

(b) perform, where appropriate, vulnerability scans and record evidence of the results of the scans, at planned intervals;

(c) address, without undue delay, vulnerabilities identified by the relevant entities as critical to their operations;

(d) ensure that their vulnerability handling is compatible with their change management, security patch management, risk management and incident management procedures;

(e) lay down a procedure for disclosing vulnerabilities in accordance with the applicable national coordinated vulnerability disclosure policy.

GUIDANCE

- As a minimum, address vulnerabilities assigned to higher classifications (e.g. 'critical' and 'high' in the CVSS) or equivalent (e.g. as defined by the national CSIRT) without undue delay. Where possible, accepting the risk of such vulnerabilities and not addressing them is not advisable.
- Share information obtained from technical vulnerability scans with designated personnel throughout the entity and with authorities to help eliminate similar vulnerabilities in other information systems.
- Disclose as yet unknown vulnerabilities to designated CSIRTs in accordance with national coordinated vulnerability disclosure (CVD) policies, where applicable.
- Identify a single point of contact and channels for communication with suppliers and service providers about issues related to network and information security.

EXAMPLES OF EVIDENCE

- Logs of a vulnerability assessed as critical to check if it was addressed.
- Licences or subscriptions for vulnerability-scanning tools.
- Configuration files of the vulnerability-scanning tools to ensure they are set up to scan the entire relevant infrastructure and are updated with the latest vulnerability definitions.
- Logs from vulnerability management tools showing scan schedules, results and follow-up actions.
- Documented technical vulnerability scan reports.
- SIEM and EDR/XDR logs for records of detected vulnerabilities and related alerts from monitoring channels.
- Reports from third-party security assessments or penetration tests.
- For vulnerabilities assessed as critical, evidence that findings from these assessments have been addressed.
- Records of any vulnerabilities disclosed, in accordance with the national CVD policy.

- Interview with the single point of contact and channels for communication with suppliers and service providers about information-security-related issues.

6.10.3. When justified by the potential impact of the vulnerability, the relevant entities shall create and implement a plan to mitigate the vulnerability. In other cases, the relevant entities shall document and substantiate the reason why the vulnerability does not require remediation.

GUIDANCE

- Ensure comprehensive documentation of identified vulnerabilities, the associated risk assessments and any mitigation plans developed.
- Define and establish the roles and responsibilities associated with vulnerability management.
- Mitigation plans should include clear timelines, assigned responsibilities and follow-up procedures.
- All mitigation plans, along with the rationale for non-remediation decisions, should be reviewed and validated by the management body responsible for risk oversight

EXAMPLES OF EVIDENCE

- Records showing timelines and responsible employees for each remediation effort and verification of fixes.
- Records or logs of past vulnerability mitigation plans or schedules.
- Records of any vulnerability that was not addressed and the justification for not addressing it.

6.10.4. The relevant entities shall review and, where appropriate, update at planned intervals the channels they use for monitoring vulnerability information.

GUIDANCE

- Review the information from the technical-vulnerability-monitoring channels at least biannually.
- Consider inventorying sources likely to report technical vulnerabilities in the identified components and distribute updates (software publisher websites, CERT website and ENISA website) ([71]).

EXAMPLES OF EVIDENCE

- List of monitoring channels for technical vulnerabilities, including suppliers and service providers' single points of contact.
- Records of past reviews and plans for future reviews of technical vulnerability channels.
- Subscriptions to relevant vulnerability notification services, mailing lists and alert systems (e.g. CERT, vendor advisories and security forums).
- Logs that document periodic reviews of the monitoring channels to verify that they are up to date and effective.
- Records of alerts or notifications received from monitoring channels about new vulnerabilities, including how these alerts were handled and any subsequent actions taken.
- Logs that record the monitoring activities for vulnerability information, including dates and sources monitored (e.g. security advisories, vendor bulletins, threat intelligence feeds).

([71]) Cyber fundamentals, PR.IP-12, Centre for Cyber Security Belgium, available at: https://atwork.safeonweb.be/sites/default/files/2024-12/cyfun_basic_v2023-03-01_e_update_2024.pdf.

TIPS

GUIDANCE

- Create and maintain procedures for identifying, assessing, prioritising and remediating vulnerabilities.
- Make sure that suppliers and service providers report vulnerabilities in their systems or products or services that present a risk to the security of the network and information systems of the entity.
- Perform vulnerability scans and record evidence of the results of the scans, when significant incidents or significant changes to operations or risks occur.
- Where possible, consider authenticated vulnerability or an alternative method to perform in depth scans.
- Review and, where appropriate, update the channels for monitoring vulnerability information when significant incidents or significant changes to operations or risks occur.

EXAMPLES OF EVIDENCE

- Documented procedures for identifying, assessing, prioritising and remediating vulnerabilities.
- Contracts with suppliers and service providers that require technical vulnerability reporting, handling and disclosure.
- Vulnerability-related communications or reports from suppliers and service providers.
- Records of ad-hoc scans performed in response to significant incidents or changes to the infrastructure, including the dates and reasons for these scans.
- Change management logs to verify that vulnerability scans are conducted following significant incidents or changes to the infrastructure or to the threat landscape.
- Records of internal audits or reviews of the vulnerability management procedures.
- Findings and corrective actions taken from these audits.

POLICIES AND PROCEDURES TO ASSESS THE EFFECTIVENESS OF CYBERSECURITY RISK-MANAGEMENT MEASURES

7. POLICIES AND PROCEDURES TO ASSESS THE EFFECTIVENESS OF CYBERSECURITY RISK-MANAGEMENT MEASURES

7.1. For the purpose of Article 21(2), point (f) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures to assess whether the cybersecurity risk-management measures taken by the relevant entity are effectively implemented and maintained.

GUIDANCE

- Take into account industry-recognised standards when developing the policy and procedures for assessing the efficient implementation of the measures ([72]).
- Implement a policy for assessing the effectiveness of implementation of measures that is proportionate to the risk posture of the entity in line with the risk assessment.

EXAMPLES OF EVIDENCE

- Documented policy and procedures for effectiveness assessments based on good practices and standards ([73]).

7.2. The policy and procedures referred to in point 7.1. shall take into account results of the risk assessment pursuant to point 2.1. and past significant incidents. The relevant entities shall determine:
(a) what cybersecurity risk-management measures are to be monitored and measured, including processes and controls;
(b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
(c) when the monitoring and measuring is to be performed;
(d) who is responsible for monitoring and measuring the effectiveness of the cybersecurity risk-management measures;
(e) when the results from monitoring and measurement are to be analysed and evaluated;
(f) who has to analyse and evaluate these results.

GUIDANCE

- When selecting measures for assessing effectiveness of implementation take into account the cost of their implementation.
- Consider one or more of the following indicative methods for assessing the effectiveness of implementation of a measure, according to the risk-treatment plan (section 2.1):

([72]) In addition to those mentioned in the mapping table at the end of this section, consider the following:
- ISO/IEC 27004:2016, Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation.
- Information Technology Infrastructure Library (ITIL).

([73]) For example, NIST SP 800-53A available at: https://csrc.nist.gov/pubs/sp/800/53/a/r5/final.

    - self-assessment,
    - benchmarking against a measure's checklist or a standard,
    - vulnerability assessment,
    - penetration testing (e.g. internal, external, red/blue team),
    - secure code review,
    - audit (e.g. internal, external, compliance) and
    - performance monitoring.
- The assessment service can be provided by an external entity or by specially authorised employees of the entity.
    - In the case of external entities, confidentiality and non-disclosure terms should be included in the contract.
    - Internal employees should be suitably trained, based on the skills required for the objective of their role and the entity should consider their objectivity and impartiality, where possible. The entity should pay particular attention to the elements of point 2.3. of the Annex to the regulation concerning the impartiality of the employees. For instance, employees should not come from the department or division whose systems are being inspected and should not have been involved in developing the code or in installing or operating the system being audited for this purpose.
- Define key performance indicators (KPIs) to measure the effectiveness of measures including, one or more, notable examples such as (indicative, non-exhaustive list) ([74]):
    - the cost of implementation and maintenance, for example capital expenditure (CAPEX) / operational expenditure (OPEX);
    - the number of employees who have attended cybersecurity trainings ([75]);
    - the number of vulnerabilities detected;
    - time to remediation;
    - the number of incidents;
    - the number of incidents related to a change;
    - incident response times; and
    - number of non-compliances (consider the elements in point 2.2 of the Annex to the regulation concerning compliance monitoring).
- If possible, use the same KPIs for each assessment and utilize standardized templates and checklists to ensure consistency and thoroughness.
- Although the frequency of monitoring and measurement of measures, addressed in point 7.2.1 (a) of the Annex to the regulation, depends on the entity's risk assessment, the entity may follow this indicative, non-exhaustive guideline:
    - continuously monitor and measure the effectiveness of mitigating measures designed to address real-time threats (e.g. firewalls, IDS/IPS);
    - monitor and measure the effectiveness of security measures related to the threat landscape biannually (e.g. vulnerability management and incident response plans);
    - assess the overall effectiveness of all measures annually;
    - assess the effectiveness of measures related to a specific incident following that incident; and

([74]) ENISA's cybersecurity investment reports offer a good reference for measuring effectiveness of measures, for example the 2023 NIS investments report, https://www.enisa.europa.eu/publications/nis-investments-2023.
([75]) The security culture framework (CSF) is an example source of KPIs for measuring the effectiveness of training.

- assess the effectiveness of measures related to a specific system or one of its components following significant changes to this system or this component.

EXAMPLES OF EVIDENCE

- Evidence that management has received reporting on the effective implementation of the measures.
- Evidence that monitoring and measurement results are reported to the management bodies (Annex to the regulation, point 2.3.3 concerning compliance monitoring).
- Documented objectives and KPIs for the implementation of the measures.
- Documented analysis and evaluation of the results from previous evaluations.
- Logs or records from previous effectiveness assessments.
- Plans or schedules for future effectiveness assessments.
- Documented roles and responsibilities.

7.3. The relevant entities shall review and, where appropriate, update the policy and procedures at planned intervals and when significant incidents or significant changes to operations or risks.

GUIDANCE

- Review policy and procedures for the assessment of the effectiveness of the measures at least every two years, taking into account:
  - changes to the information systems;
  - changes to the environment of operation; and
  - trends related to threats and vulnerabilities (take into account root cause analysis) ([76]).
- Update the policy and procedures based on findings from security tests (Annex to the regulation, point 6.5.2 (c)) and the independent review of the policy on the security of the network and information systems (Annex to the regulation, point 2.3.3), if applicable.
- Take into account the results of the assessment and consider them when identifying and prioritising appropriate risk-treatment options and measures (Annex to the regulation, point 2.1.3).

EXAMPLES OF EVIDENCE

- Logs or records from previous policy reviews.
- Plans or schedules for future effectiveness assessment reviews.
- Risk-treatment plan that takes into account the results of the effectiveness assessments.
- Minutes from meetings where security-testing results are discussed and the effectiveness of other policies is reviewed and improvements to them are discussed based on these results.
- Records showing updates to other policies and procedures with a view to assessing their effectiveness.

([76]) More information on information security incident root cause analysis can be found in Forum of Incident Response and Security Teams, 'FIRST CSIRT services framework', Version 2.1, '6.2.4 Function: Information security incident root cause analysis', https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1#6-Service-Area-Information-Security-Incident-Management

BASIC CYBER HYGIENE PRACTICES AND SECURITY TRAINING

8. BASIC CYBER HYGIENE PRACTICES AND SECURITY TRAINING

8.1 AWARENESS RAISING AND BASIC CYBER HYGIENE PRACTICES

8.1.1. For the purpose of Article 21(2), point (g) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees are aware of risks, are informed of the importance of cybersecurity and apply cyber hygiene practices.

GUIDANCE

- Implement cybersecurity awareness programmes:
  - use various formats, such as workshops, webinars and e-learning modules;
  - use multiple communication channels (emails, newsletters and intranet) to keep employees informed about cybersecurity updates, risks and cyber hygiene practices for users.

EXAMPLES OF EVIDENCE

- Awareness raising programme, for example a comprehensive outline of the programme, detailing its objectives, content, frequency, syllabus and schedule.

8.1.2. For the purpose of point 8.1.1., the relevant entities shall offer to all employees, including members of management bodies, as well as to direct suppliers and service providers where appropriate in accordance with point 5.1.4, an awareness raising programme, which shall:
(a) be scheduled over time, so that the activities are repeated and cover new employees;
(b) be established in line with the network and information security policy, topic-specific policies and relevant procedures on network and information security;
(c) cover cybersecurity risk-management measures in place, contact points and resources for additional information and advice on cybersecurity matters, as well as cyber hygiene practices for users.

GUIDANCE

- Include cyber hygiene practices ([77]) for relevant users (indicative, non-exhaustive list):
  - clear desk and screen policy,
  - use of relevant strong authentication means and methods, multi factor passwords etc,
  - event reporting,
  - safe email use and web browsing,
  - protection from phishing and social engineering,
  - secure use of mobile devices,
  - secure use of the entity's connected-vehicles,
  - secure connection practices,

([77]) Refer to recitals 49, 50 and 89 of the NIS2 Directive for clarifications of the term 'cyber hygiene'.

    - backup practices,
    - zero-trust concept,
    - software updates,
    - secure device configuration,
    - network segmentation,
    - secure teleworking practices.
- Include the following in the programme (indicative, non-exhaustive list).
    - Train personnel on the policy on the security of network and information systems.
    - Train personnel to recognize social engineering attacks, such as phishing, pre-texting and tailgating.
    - Train personnel to be aware of causes of unintentional data exposure. Example topics include the erroneous delivery of sensitive data, losing a portable end-user device, providing unauthorized access to an entity's connected-vehicle and the data stored on it and publishing data to unintended audiences.
    - Train personnel on the dangers of connecting to and transmitting data via insecure networks for the entity's activities. If the entity has remote workers, training should include guidance to ensure that all users securely configure their home network infrastructure.
    - Train personnel in understanding malicious and unauthorised software, on the importance of malicious software detection and on the risks and consequences of using unauthorised software.
- Offer employees contact points and resources for additional advice.
- To implement the awareness raising programme, consult available sources, such as those from national or international cybersecurity organisations, ENISA's AR-in-a-Box ([78]) and the Cybersecurity Skills Academy ([79]).

EXAMPLES OF EVIDENCE

- Awareness raising programme, that is, a comprehensive outline of the programme, detailing its objectives, content, frequency, syllabus and schedule.
- Copies of the awareness-raising materials distributed to employees, including handouts, emails, presentations and online modules.
- Logs, sign-in sheet, certificates of completion or acknowledgements given to employees upon completing the programme, showing which employees have taken part in the awareness-raising programme.

8.1.3. The awareness raising programme shall, where appropriate, be tested in terms of effectiveness. The awareness raising programme shall be updated and offered at planned intervals taking into account changes in cyber hygiene practices, and the current threat landscape and risks posed to the relevant entities.

GUIDANCE

- Offer cybersecurity awareness raising programmes periodically.

([78]) https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box.
([79]) Communication from the Commission to the European Parliament and the Council – Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy'), COM(2023) 207 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A207%3AFIN.

- Test the effectiveness of the awareness raising programme for example by using quizzes or real scenarios.
- Consider common KPIs (Annex to the regulation, point 7.2) to measure the effectiveness of the awareness-raising programme.
- Review and update the awareness-raising programme at least annually.

EXAMPLES OF EVIDENCE

- Logs, sign-in sheets, certificates of completion or acknowledgements given to employees upon completing the programme showing which employees have taken part in the awareness-raising programme.
- Results from any quizzes or assessments conducted to measure the employees' understanding of the topics covered.
- Employee feedback forms on the awareness raising programme, which can provide insight into the effectiveness of the programme and areas for improvement.
- Reviewed and updated records showing that the programme is reviewed regularly and updated as necessary.

8.2 SECURITY TRAINING

8.2.1. The relevant entities shall identify employees, whose roles require security relevant skill sets and expertise and ensure that they receive regular training on network and information system security.

GUIDANCE

- Assess which roles within the entity require security-relevant skills and expertise.
- Offer training that focuses on the specific security skills required by the identified roles.
- Consider globally recognized qualifications and certifications, and the ECSF ([80]).

EXAMPLES OF EVIDENCE

- A comprehensive outline of the training programme, detailing the objectives for different roles and how to reach them, content and frequency of the training.

8.2.2. The relevant entities shall establish, implement and apply a training program in line with the network and information security policy, topic-specific policies and other relevant procedures on network and information security which lays down the training needs for certain roles and positions based on criteria.

GUIDANCE

- Provide role-specific network and information security training ([81]).
- Consider various training methods, such as online courses, workshops, hands-on labs and simulations.
- Consider various types of training, such as courses, certifications or attending security conferences or webinars, and the maintenance of certifications.

([80]) https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf.
([81]) https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf.

- Examples of training may include secure system administration courses for IT professionals, Open Worldwide Application Security Project® awareness and prevention training for web application developers and advanced social engineering awareness training for high-profile roles.

EXAMPLES OF EVIDENCE

- A comprehensive outline of the training programme, detailing the objectives for different roles and how to reach them, content and frequency of the training.
- Assessment of effect and feedback from trainings.

8.2.3. The training referred to in point 8.2.1. shall be relevant to the job function of the employee and its effectiveness shall be assessed. Training shall take into consideration security measures in place and cover the following:
(a) instructions regarding the secure configuration and operation of the network and information systems, including mobile devices;
(b) briefing on known cyber threats;
(c) training of the behaviour when security-relevant events occur.

GUIDANCE

- Topics to include in the programme may include the following (indicative, non-exhaustive list).
  - Train personnel in authentication best practices, such as MFA, password creation and credential management.
  - Train personnel in how to identify and properly store, transfer, archive and destroy sensitive data.
  - Train personnel to recognise a potential incident, such as unusual email attachments, unexpected system behaviour and suspicious network traffic.
  - Train personnel in how to report events promptly and accurately, including the use of designated communication channels.
  - Train personnel to understand how to verify and report out-of-date software or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.
  - Train relevant personnel in crisis management and business continuity procedures. Incorporate simulated events ([82]) into crisis management training to facilitate an effective response by personnel in crisis situations.
  - Train relevant personnel (e.g. system administrators and software developers) in the secure configuration and operation of the network and information systems. Provide regular updates on the latest cyber threats.
- Test the security knowledge of employees to make sure that it is sufficient and up to date.

EXAMPLES OF EVIDENCE

- Comprehensive outline of the training programme, detailing the objectives of different roles and how to reach them, and the content and frequency of the training.
- Results from any quizzes or assessments conducted to measure the employees' understanding of the topics covered.

([82]) In its simplest form, the exercise can mean simulating the continuity and recovery procedures through discussion (known as a tabletop exercise).

8.2.4. The relevant entities shall apply training to staff members who transfer to new positions or roles which require security relevant skill sets and expertise.

GUIDANCE

- Examine whether the new position or role of an employee requires role-specific network and information security training.

EXAMPLES OF EVIDENCE

- Logs, sign-in sheets, certificates of completion or acknowledgements given to employees upon completing the training, showing that employees who transferred to new positions or roles attended training sessions relevant to the new position or role.
- Evidence of maintenance of certifications obtained.

8.2.5. The program shall be updated and run periodically taking into account applicable policies and rules, assigned roles, responsibilities, as well as known cyber threats and technological developments.

GUIDANCE

- Provide cybersecurity training periodically.
- Review and update the training programme at least annually.

EXAMPLES OF EVIDENCE

- Logs, sign-in sheets, certificates of completion or acknowledgements given to employees upon completing the training, showing which employees attended the training sessions.
- Information materials distributed to employees, including handouts, presentations and online modules.
- Updates showing that the training programme is reviewed and updated regularly to keep up with the latest cybersecurity threats and best practices.
- Employee feedback forms on the training sessions, which can provide insight into the effectiveness of the training and areas for improvement.

TIP

GUIDANCE

- Encourage participation in threat-intelligence-sharing communities to stay informed about emerging threats.

CRYPTOGRAPHY

9. CRYPTOGRAPHY

9.1. For the purpose of Article 21(2), point (h) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures related to cryptography, with a view to ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of data in line with the relevant entities' asset classification and the results of the risk assessment carried out pursuant to point 2.1.

GUIDANCE

- Ensure that the comprehensive policy and procedures related to cryptography are in line with relevant regulations and state-of-the-art standards ([83]).

EXAMPLES OF EVIDENCE

- Documented policy on cryptography and procedures related to cryptography.

9.2. The policy and procedures referred to in point 9.1 shall establish:
(a) in accordance with the relevant entities' classification of assets, the type, strength and quality of the cryptographic measures required to protect the relevant entities' assets, including data at rest and data in transit;
(b) based on point (a), the protocols or families of protocols to be adopted, as well as cryptographic algorithms, cipher strength, cryptographic solutions and usage practices to be approved and required for use in the relevant entities, following, where appropriate, a cryptographic agility approach;
(c) the relevant entities' approach to key management, including, where appropriate, methods for the following:
(i) generating different keys for cryptographic systems and applications;
(ii) issuing and obtaining public key certificates;
(iii) distributing keys to intended entities, including how to activate keys when received;
(iv) storing keys, including how authorised users obtain access to keys;
(v) changing or updating keys, including rules on when and how to change keys;
(vi) dealing with compromised keys;
(vii) revoking keys including how to withdraw or deactivate keys;
(viii) recovering lost or corrupted keys;
(ix) backing up or archiving keys;
(x) destroying keys;
(xi) logging and auditing of key management-related activities;
(xii) setting activation and deactivation dates for keys ensuring that the keys can only be used for the specified period of time according to the organization's rules on key management.

([83]) Non-exhaustive list of standards:
- NIST special publications: SP 800-175A, SP 800-175B, SP 800-56A/B, SP 800-57;
- Federal Information Processing Standards 197, 202, 186-4;
- ISO/IEC: 19790, 18033;
- BSI TR-02102-1 'Cryptographic Mechanisms: Recommendations and Key Lengths', Version: 2025-1, January 31, 2025.

GUIDANCE

- Ensure that the policy and procedures cover cryptographic mechanisms, such as digital signatures ([84]) and hashes ([85]), to:
  - protect the confidentiality and integrity of data in transit and at rest;
  - detect unauthorized changes to data at rest marked as critical; and
  - ensure secure disposal of the data after its lawful use.
- Set up a mechanism (either manual or automated) for the selection, establishment and management (including updating) of cryptographic keys.
- Apply encryption in sensitive information transfer (e.g. key generation and key management).
- Consider the encryption of electronic media that contain confidential/sensitive information.
- Ensure the confidentiality and integrity of the data with cryptographic mechanisms, when, for example (indicative, non-exhaustive list):
  - sharing information;
  - scanning network traffic;
  - using secure online (e.g. client-side cloud encryption) and offline storage; and
  - removing sensitive data from storage media.
- Maintain availability of information in the event of the loss of cryptographic keys, for example by escrowing encryption keys.
- Produce, control and distribute symmetric and asymmetric cryptographic keys using key management technology and processes.
- Consider automated cryptographic key management mechanisms to:
  - generate keys for different cryptographic systems and different applications;
  - generate and obtaining public key certificates;
  - distribute keys to intended users; and
  - deal with compromised keys.
- Keep logs of cryptographic key management activities to ensure accountability, traceability and support for incident response and audit activities. As a minimum, logging should include key generation or renewal, key transmission and key destruction or revocation.
- Where applicable, key retrieval, archiving and storage activities should also be logged, particularly in environments where manual handling or high-assurance key protection is required.
- Ensure the protection of cryptographic keys against modification and loss.
- Ensure the protection of secret and private keys against unauthorized use and disclosure.
- Ensure the authenticity of public keys.
- Physically protect equipment used to generate, store and archive keys.
- Limit the use of ad hoc cryptographic processes.
- Consider, where appropriate, a cryptographic agility approach ([86]). Key features of this approach are:
  - flexibility in algorithm selection;

([84]) Key digital signature use case areas are (indicative, non-exhaustive list): document/software code signing, authentication, data integrity and workflow automation and compliance.
([85]) Use cases for the use of secure hash algorithms are (indicative, non-exhaustive list): backup integrity, secure password storage, log integrity.
([86]) Cryptographic agility, or crypto-agility, is the ability of a system to quickly and seamlessly switch between different cryptographic algorithms and protocols without significant changes to the system's infrastructure. For example, the X.509 public key certificate system demonstrates crypto-agility by allowing the use of different cryptographic parameters, such as key types and hash algorithms.

- modular design of the architecture whereby cryptographic components can be changed or updated independently without affecting the entire system;
- regular updates and patching;
- compliance with the legislative frameworks and governance of the use of cryptography within the entity's networks and information systems;
- future-proofing by considering quantum cryptographic algorithms.

- Consider evaluating the chosen encryption methods to verify that they meet industry standards for secure methods ([87]).

EXAMPLES OF EVIDENCE

- Documented policy on cryptography in line with relevant regulations and state-of-the-art standards.
- Documented guidelines for encryption.
- Acceptable encryption algorithms, key lengths, protocols ([88]) or family of protocols ([89]) in line with the state of the art.
- Safeguards to protect the secrecy of secret (private) key(s) in place.
- Evidence of the existence of cryptographic mechanisms that support ensuring the confidentiality and integrity of the data at rest and in transit.
- Evidence of the existence of a mechanism (either manual or automated) for the establishment and management of cryptographic keys.
- Evidence of encryption implementation on various systems (e.g. databases, files, communications).
- Access control mechanisms for cryptographic keys and encrypted data.
- Verification that access is restricted to authorized personnel and that actions related to cryptographic keys are logged and monitored.
- Assessments of cryptographic measures for protecting data privacy.
- Evidence of secure key generation.
- Internal or external audit reports focusing on cryptographic measures.
- Evidence that the entity follows cryptographic best practices, including documentation of how new best practices are identified and incorporated.

9.3. The relevant entities shall review and, where appropriate, update their policy and procedures at planned intervals, taking into account the state of the art in cryptography.

GUIDANCE

- Ensure the cryptography policy aligns with relevant industry standards and with advancements in the field.
- Review the cryptography policy and procedures at least annually.
- Maintain a procedure that specifies how reviews of the cryptography policy and procedures are conducted, including responsible personnel and review intervals.

([87]) For example NIST 800-175 and 800-57.
([88]) A cryptographic protocol is a set of rules and procedures that use cryptographic algorithms to achieve specific security objectives in communication and data exchange. Examples of such protocols are secure sockets layer / transport layer security (SSL/TLS) and secure shell protocol (SSH).
([89]) A family of cryptographic protocols is a group of related protocols that share common cryptographic techniques and principles to achieve various security objectives. Examples are (a) key establishment (e.g. Diffie-Helman and RSA), (b) identification (e.g. Kerberos), (c) message authentication (e.g. hash-based message authentication code), (d) secret sharing (e.g. Shamir's Secret Sharing) and (e) zero knowledge proof (e.g. Schnorr) protocols.

- Ensure that changes to the cryptographic measures are tested before being applied.
- Ensure that changes to the cryptographic measures are communicated to employees.

EXAMPLES OF EVIDENCE

- Logs of changes made to the cryptography policy and procedures
- Test plans and results that demonstrate the implementation and effectiveness of updated cryptographic measures.
- Records of notifications or reminders sent to relevant personnel about upcoming reviews of the cryptography policy and procedures.
- Communication records informing personnel about updates to the cryptography policy following advancements in the field or significant changes.
- Evidence that the entity remains up to date with the latest developments in cryptography (e.g. member of cryptographic bodies or consortia (e.g. Internet Engineering Task Force and cryptographic research groups) and subscriptions to cryptographic journals/feeds, mailing lists or news feeds).

TIPS

GUIDANCE

- Train employees and make them aware of the use of cryptographic measures in the entity.
- Make sure network and information systems automatically encrypt and secure all portable and removable media.
- Where appropriate, consider implementing a key management system to ensure the secure handling of cryptographic keys.

EXAMPLES OF EVIDENCE

- Records of training programmes related to cryptography for employees.
- Employees aware of the confidentiality and integrity of data, communications and procedures and what they imply for their work.
- Employees handling sensitive information aware of and understanding the cryptography policies and procedures.
- Key management system in place.

Chapter 10

HUMAN RESOURCES SECURITY

10. HUMAN RESOURCES SECURITY

10.1 HUMAN RESOURCES SECURITY

10.1.1. For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees and direct suppliers and service providers, wherever applicable, understand and commit to their security responsibilities, as appropriate for the offered services and the job and in line with the relevant entities' policy on the security of network and information systems.

GUIDANCE

- Define clear security roles and responsibilities for employees, aligned with the entity's security policies and each employee's functional role. Define relevant security responsibilities for direct suppliers and service providers, within the scope of contractual obligations, ensuring they are appropriate to the nature of the services provided and aligned with the entity's overall security requirements.
- Establish onboarding and continuous education programmes that include both security awareness and role-specific cybersecurity training tailored to different risk exposures.
- Implement periodic assessments to evaluate understanding of security responsibilities, supported by mandatory refresher training as needed.
- Ensure that security responsibilities are formally documented and integrated into job descriptions, contractual agreements and performance review processes. Incorporate relevant security responsibilities into contractual agreements or service-level agreements (SLA), for direct suppliers and service providers with clear language regarding expectations and compliance requirements.
- Promote a culture of accountability by requiring formal acknowledgement of security obligations and by linking compliance to incentives and disciplinary measures, where appropriate.
- Develop and maintain a centralized repository of training records, acknowledgements, certifications and contractual clauses to demonstrate compliance and facilitate audits.
- Require suppliers and service providers to designate responsible contacts for cybersecurity and encourage or mandate participation in relevant security briefings or training programmes provided by the entity.

EXAMPLES OF EVIDENCE

- List of employees whose roles require specific security skills and their assignment to roles.
- Documented evidence of regular training sessions on security of network and information systems for employees, direct suppliers and service providers, wherever applicable. This includes attendance records, training materials and feedback forms.
- Signed acknowledgements from employees, direct suppliers and service providers, wherever applicable, confirming they have read, understood and agreed to comply with the policy.
- Reports from internal or external audits assessing the understanding and implementation of security responsibilities among employees, direct suppliers and service providers, wherever applicable.
- Inclusion of security responsibilities, where relevant, in employee performance reviews and evaluations.

- Contracts with direct suppliers and service providers that include clauses on security responsibilities and compliance with the entity's policies or written justifications by the direct supplier or service provider in cases where these clauses do not exist in the contract.
- Certifications or attestations of cybersecurity skills from nationally recognized or accredited bodies confirming that a person fulfils specific requirements regarding cybersecurity knowledge and skills.

10.1.2. The requirement referred to in point 10.1.1. shall include the following:

(a) mechanisms to ensure that all employees, direct suppliers and service providers, wherever applicable, understand and follow the standard cyber hygiene practices that the entities apply pursuant to point 8.1.;

(b) mechanisms to ensure that all users with administrative or privileged access are aware of and act in accordance with their roles, responsibilities and authorities;

(c) mechanisms to ensure that members of management bodies understand and act in accordance with their role, responsibilities and authorities regarding network and information system security;

(d) mechanisms for hiring personnel qualified for the respective roles, such as reference checks, vetting procedures, validation of certifications or written tests.

GUIDANCE

- Implement regular awareness raising on cyber hygiene practices for users, tailored to different roles and responsibilities (Annex to the regulation, point 8.1). Wherever applicable, require employees of direct suppliers and service providers, to follow similar awareness raising on cyber hygiene via contractual clauses.
- Communicate clear and concise cyber hygiene practices for users to all employees, suppliers and service providers. Require acknowledgement of receipt and understanding (Annex to the regulation, point 8.1).
- Consider specialised training for users with administrative or privileged access, focusing on their specific responsibilities (Annex to the regulation, point 8.2).
- Establish performance metrics related to security responsibilities and include them in management evaluations.
- Hold regular briefings for members of management bodies on the importance of network and information system security, their specific responsibilities and the potential impact of incidents (section 8.2).
- Conduct thorough reference checks, where appropriate, to verify the candidate's previous experience and performance in similar roles.
- Consider vetting procedures, including background checks (section 10.2), to ensure the candidate's suitability for the role.
- Validate any relevant certifications claimed by the candidate, to ensure they are current and legitimate.
- Use written tests or practical assessments to evaluate the candidate's knowledge and skills related to network and information system security.
- Use interview panels, where appropriate, that also include security experts, to assess the candidate's technical and behavioural competencies.

EXAMPLES OF EVIDENCE

- Training and awareness raising material such as videos, slides, emails, newsletters, posters and intranet announcements.

- Documented records showing that all users with administrative or privileged access were properly informed and are aware of and are following their network and information security roles, responsibilities and authorities.
- Contractual agreements, the policy on the security of network and information systems, terms and conditions, code of conduct and other documentation confirming that all users have understood and are following the standard cyber hygiene practices for users (signed employment contracts and any proof of employees having been informed of their responsibilities relating to network and information security).
- Records of security training sessions provided to employees, including attendance logs and training schedules.
- Evidence, for example attendance certificates where relevant, that suppliers and service providers receive security training relevant to their roles.
- Mechanisms for hiring qualified personnel (e.g. reference check, validation of certifications and written tests) in place.
- Use of relevant cybersecurity frameworks and standards along with widely recognised quality management and capability maturity models and standards.

10.1.3. The relevant entities shall review the assignment of personnel to specific roles as referred to in point 1.2., as well as their commitment of human resources in that regard, at planned intervals and at least annually. They shall update the assignment where necessary.

GUIDANCE

- Set up a formal schedule for reviewing personnel assignments and resource commitments. This should occur at least annually.

EXAMPLES OF EVIDENCE

- Up-to-date list of employees and their assignment to roles.
- Records of the review process, including the criteria used, the findings and any changes made.

10.2 VERIFICATION OF BACKGROUND

10.2.1. The relevant entities shall ensure to the extent feasible verification of the background of their employees and where applicable of direct suppliers and service providers in accordance with point 5.1.4, if necessary for their role, responsibilities and authorisations.

GUIDANCE

- Identify which roles, responsibilities and authorities require verification of background, based on the criteria in point 10.2.2 (a) of the Annex to the regulation.
- Perform background verification on employees and, where applicable, direct suppliers and service providers in accordance with point 5.1.4 (c) of the Annex to the regulation.

EXAMPLES OF EVIDENCE

- Documented background verification process.
- Results of background verification on employees and, where applicable, direct suppliers and service providers in accordance with point 5.1.4 (c).

10.2.2. For the purpose of point 10.2.1., the relevant entities shall:

(a) put in place criteria, which set out which roles, responsibilities and authorities shall only be exercised by persons whose background has been verified;

(b) ensure that verification referred to in point 10.2.1 is performed on these persons before they start exercising these roles, responsibilities and authorities, which shall take into consideration the applicable laws, regulations and ethics in proportion to the business requirements, the asset classification as referred to in point 12.1. and the network and information systems to be accessed and the perceived risks.

GUIDANCE

- Where applicable, define criteria for roles, responsibilities and authorities that will be exercised only by persons who have undergone background verification. An indicative, non-exhaustive list is the following:
  - executives and senior management,
  - roles with access to sensitive information,
  - roles with financial responsibilities,
  - roles involving procurement and vendor management,
  - roles that grant access to physical assets or are responsible for physical security.
- Define criteria and limitations for background verification (e.g. who is eligible to screen people, and how, when and why verification reviews are carried out).
- For background verification, consider checking the criminal records of the person concerned with regard to offences that would be relevant to a specific position.
- Ensure that checks of criminal records align with legal and regulatory requirements (e.g. national (labour) laws and the GDPR).
- Collect and handle information on job candidates, taking into consideration any applicable laws, regulations and ethics, including the protection of personal data. This may include collecting professional references.
- Consider screening requirements in the contractual agreements between the entity and the direct suppliers and service providers in cases of personnel contracted with an external supplier.
- Periodically repeat verification to confirm the ongoing suitability of personnel, depending on the criticality of a person’s role, responsibilities and authorities.
- Entities should be permitted to rely on background checks of contractors employed by a third-party talent agency with which the entity covered has contracts for performing services.

EXAMPLES OF EVIDENCE

- Records of an analysis conducted to determine which roles, responsibilities and authorities require background verification.
- Guidance for employees about when/how to perform background verification.
- Records of completed verifications of professional references for employees or, where applicable, for direct suppliers and service providers.
- Signed consent forms from employees or job candidates, confirming their agreement to undergo background verification.
- Documentation of follow-up actions taken in response to any issues or discrepancies identified during background verification.
- Agreements with third-parties that perform background verification services, if used, to ensure they comply with legal and policy requirements.

10.2.3. The relevant entities shall review and, where appropriate, update the policy at planned intervals and update it where necessary.

GUIDANCE

- Where necessary, review and update background verification procedure at least annually.

EXAMPLES OF EVIDENCE

- Records of background verification for roles requiring ongoing clearance.
- Review comments or change logs of the procedure.

10.3 TERMINATION OR CHANGE OF EMPLOYMENT PROCEDURES

10.3.1. The relevant entities shall ensure that network and information system security responsibilities and duties that remain valid after termination or change of employment of their employees are contractually defined and enforced.

GUIDANCE

- Include specific clauses in employment contracts that outline the ongoing security responsibilities and duties of employees after their employment ends or their role changes.

EXAMPLES OF EVIDENCE

- Documents, such as terms and conditions of employment, contracts or agreements, outlining responsibilities and duties still valid after termination of employment or contract.

10.3.2. For the purpose of point 10.3.1., the relevant entities shall include in the individual's terms and conditions of employment, contract or agreement the responsibilities and duties that are still valid after termination of employment or contract, such as confidentiality clauses.

GUIDANCE

- Ensure these clauses cover the protection of confidential information, return of company property and restrictions on accessing the entity's network and information systems.
- Revoke access to network and information systems in a timely manner upon termination or role change.
- Identify and document all assets to be returned upon termination or change of employment.
- After a change of employment, brief and inform personnel on the procedures in place.

EXAMPLES OF EVIDENCE

- Records confirming the timely return of the entity's assets.
- Records confirming the timely revocation of access rights.
- Copies of written notifications to the employee about the termination of or change in employment status.

TIPS

GUIDANCE

- Identify and transfer to another individual network and information security roles and responsibilities held by any individual who leaves the organisation.
- Where deemed reasonably necessary, conduct thorough exit interviews to remind departing employees of their ongoing security responsibilities.

- Collect company property and revoke access to systems.
- Monitor for any unauthorized access attempts by former employees. Use security tools to detect and respond to suspicious activities. Maintain logs of access attempts and investigate any anomalies.
- Regularly review and update policies related to post-employment security responsibilities to ensure they remain effective and aligned with current legal and regulatory requirements. Keep a record of changes and ensure that it is up to date.
- Take into account changes or past incidents when reviewing the process
- Involve legal and human resources (HR) departments in the review process to ensure comprehensive coverage.

EXAMPLES OF EVIDENCE

- Records of all contractual agreements, non-disclosure agreements, exit interviews and access revocations, and any legal action taken.
- Documentation showing that the process is reviewed regularly and updated as necessary.
- Evidence that the employee's access to the entity's systems and facilities has been revoked or altered in accordance with a process.
- Documentation of the process for personnel changes, including responsibilities for managing changes, description of rights of access and possession of assets for each role, and procedures for briefing and training personnel in new roles (e.g. standardised checklists used during the termination process to ensure all necessary steps are taken).

10.4 DISCIPLINARY PROCESS

10.4.1. The relevant entities shall establish, communicate and maintain a disciplinary process for handling violations of network and information system security policies. The process shall take into consideration relevant legal, statutory, contractual and business requirements.

GUIDANCE

- Make sure that the process holds employees accountable for violations of the network and information system security policies.
- Involve human resources in implementing the disciplinary process, ensuring it aligns with legal and regulatory requirements (e.g. national labour laws and the GDPR).
- Communicate and raise awareness of the process among employees.
- Protect the identity of individuals subject to disciplinary action, where possible, in line with applicable requirements.

EXAMPLES OF EVIDENCE

- Disciplinary process documentation outlining the types of violations that may be subject to disciplinary actions, and what steps to take when a violation occurs.
- Evidence that the policy has been communicated to all employees, which could include email records, meeting minutes or training session materials.
- Records of any violations of the network and information system security policies that have occurred and the corresponding disciplinary actions taken, demonstrating adherence to the disciplinary process. Examples of such records may include interviews with employees, witness statements, e-mails, paperwork, digital records, system logs and phone records.

10.4.2. The relevant entities shall review and, where appropriate, update the disciplinary process at planned intervals and when necessary due to legal changes or significant changes to operations or risks.

GUIDANCE

- Regularly review and update the disciplinary process at planned intervals and promptly when legal changes or significant operational or risk changes occur.

EXAMPLES OF EVIDENCE

- Records of reviews and updates showing that the disciplinary process is reviewed regularly and updated as necessary.

TIPS

GUIDANCE

- Include the disciplinary process for handling violations of network and information system security policies in the entity's overall disciplinary process, if available.
- Recognize that deliberate violations of the policy on the security of network and information systems may require immediate actions.
- Do not initiate the disciplinary process without verifying that a violation of network and information system security policies has occurred.
- Consider the following factors for the process:
  - the nature (who, what, when, how) and gravity of the violation and its consequences;
  - whether the offence was intentional (malicious) or unintentional (accidental);
  - whether this is a first or repeated offence;
  - whether or not the employee who committed the violation was properly trained.
- Use the process as a deterrent to prevent employees from violating the network and information system security policies.
- Reward individuals who demonstrate excellent behaviour regarding network and information security as a means of promoting and encouraging good behaviour.

EXAMPLES OF EVIDENCE

- Disciplinary process documentation outlining the types of violations that may be subject to disciplinary actions, and what steps to take when a violation occurs.

ACCESS CONTROL

11. ACCESS CONTROL

11.1 ACCESS CONTROL POLICY

11.1.1. For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall establish, document and implement logical and physical access control policies for the access to their network and information systems, based on business requirements as well as network and information system security requirements.

GUIDANCE

- Implement and maintain logical and physical access restrictions to network and information system based on access-control policies that take into account industry good practices.
- Ensure that these policies are documented, communicated to all relevant stakeholders and include clear guidelines on the appropriate use of access privileges.

EXAMPLES OF EVIDENCE

- Access control policy document or documents outlining the access control requirements, procedures and responsibilities.

11.1.2. The policies referred to in point 11.1.1. shall:

(a) address access by persons, including staff, visitors and external entities such as suppliers and service providers;

(b) address access by network and information system processes;

(c) ensure that access is only granted to users that have been adequately authenticated.

GUIDANCE

- Implement access control rules by defining and mapping appropriate access rights and restrictions to human users or network and information system processes (e.g. a machine, device or a service). To simplify access control management, assign specific roles to groups.
    - Access control rules can be implemented in different granularities, ranging from covering whole networks or systems to specific data fields and can also consider properties, such as user location or the type of network connection that is used for access.
    - Use business requirements and risk assessment results to define which access control rules are applied and which granularity is required.
- Take into account the following when defining and implementing access control rules:
    - consistency between access rights and asset classification;
    - consistency between access rights and physical perimeter security needs and requirements;
    - consideration of all types of available connections in distributed environments so entities are only provided with access to associated assets, including networks and network services, that they are authorized to use;
    - consideration of how elements or factors relevant to dynamic access control can be reflected.
- Develop documented procedures and defined responsibilities to support the access control rules.

EXAMPLES OF EVIDENCE

- Access control policy document outlining the access control requirements, procedures and responsibilities.

- User access records showing the list of users and their corresponding levels of access to various network and information systems.
- Authentication protocols, meaning documentation of the authentication methods in place, such as MFA.
- Authorization mechanisms with details on how permissions are granted, reviewed and revoked, ensuring that access rights are in line with users' roles, responsibilities and authorities.
- Access logs that record user access activities, which can be used to track and audit user behaviour within the system in the event of suspected misconduct.
- Access rights review records showing alignment with asset classifications.
- Records of access control assessments that align access rights with physical security requirements.
- Network diagrams showing access control measures for different connection types and network access control policies.
- Logs showing dynamic access control decisions based on user behaviour or environment factors

11.1.3. The relevant entities shall review and, where appropriate, update the policies at planned intervals and when significant incidents or significant changes to operations or risks occur.

GUIDANCE

- Review the policies at least annually.

EXAMPLES OF EVIDENCE

- Past incident reports with records of any security incidents related to access control, including unauthorized access attempts and the responses to such events.
- Change management records of any changes made to access rights, showing adherence to the policy during modifications.
- Records of reviews and updates showing that the policies are reviewed regularly and updated as necessary.
- Reports from internal or external audits that assess the effectiveness of and compliance with the access control policy.

TIPS

GUIDANCE

- Consider the two overarching principles most frequently used in the context of access control:
  - need-to-know: an entity is only granted access to the information that it requires to perform its tasks and in line with the asset classification levels of point 12.1 of the Annex to the regulation (different tasks or roles mean different need-to-know information and hence different access profiles);
  - need-to-use: an entity is only assigned access to information technology infrastructure where a clear need is present.
- Consider the following when specifying access control rules:
  - establishing rules based on the premise of least privilege ('everything is generally forbidden unless expressly permitted') rather than the weaker rule ('everything is generally permitted unless expressly forbidden');

    - changes in user permissions that are initiated automatically by the network and information system and those initiated by a system administrator;
    - when to define and regularly review the approval.
- Consider ways to implement access control, such as mandatory access control (MAC), discretionary access control (DAC), role-based access control (RBAC) and attribute-based access control (ABAC) depending on the business needs of the organisation.
- Take into account the fact that access control rules can also contain dynamic elements (e.g. a function that evaluates past accesses or specific environmental values).

EXAMPLES OF EVIDENCE

- Access control policy document outlining the access control requirements, procedures and responsibilities.
- Access reviews showing adherence to need-to-know and need-to-use principles.
- Change management records of any changes made to access rights, showing adherence to the policy during modifications.
- Access control system configurations showing the adoption of MAC, DAC, RBAC or ABAC depending on business needs.

11.2 MANAGEMENT OF ACCESS RIGHTS

11.2.1. The relevant entities shall provide, modify, remove and document access rights to network and information systems in accordance with the access control policy referred to in point 11.1.

11.2.2. The relevant entities shall:

(a) assign and revoke access rights based on the principles of need-to-know, least privilege and separation of duties;

(b) ensure that access rights are modified accordingly upon termination or change of employment;

(c) ensure that access to network and information systems is authorised by the relevant persons;

(d) ensure that access rights appropriately address third-party access, such as visitors, suppliers and service providers, in particular by limiting access rights in scope and in duration;

(e) maintain a register of access rights granted;

(f) apply logging to the management of access rights.

GUIDANCE

- Ensure each user only has access to information necessary for their role (‘need-to-know’).
- Restrict user permissions to the minimum necessary for their duties (‘least privilege’). Regularly review and adjust access rights as needed.
- Determine which duties and areas of responsibility need to be segregated. Establish and follow a process for requesting and approving access, preferably automated. The process should:
    - cover granting access rights to assets upon the new hire or role change of a user;
    - obtain authorization from the owner of the asset, separate approval for access rights by management bodies can also be appropriate;
    - ensure that access rights are activated (e.g. by service providers) only after authorization procedures are successfully completed;
    - consider the business requirements and the entity’s access control policy;
    - consider segregation of duties, including segregating the roles of approval and implementation of the access rights and separation of conflicting roles;

- verify that the level of access granted is in accordance with the access control policy and is consistent with other information security requirements such as segregation of duties;
- consider giving temporary access rights for a time and revoking them at the expiry date, in particular for temporary personnel or temporary access required by personnel.

- Establish and follow a process, preferably automated, for revoking access to assets. The process should:
  - timely disable accounts upon the termination, rights revocation or role change of a user, as needed; disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails;
  - modify the access rights of users who have changed roles or jobs;
  - remove or adjust access rights, which can be done by removing, revoking or replacing keys, authentication information, identification cards or subscriptions.
  - where feasible, enable different components or services to share information (signals) about access revocation in a timely manner.
- Limit third-party access based on need and duration. Use temporary access accounts with expiry dates and regularly review third-party access rights.
- Ensure third parties acknowledge their access responsibilities and obligations.
- Where appropriate ([90]), keep a detailed and up-to-date central record (register or database) of all granted access rights, including user names, roles, permissions and dates of access changes.
- Establish and maintain an inventory of the authentication and authorization systems, including those hosted on-site or with a remote service provider.
- Implement logging for all access rights management activities. Logs should include details of who granted or modified access, when and what changes were made.
- Minimise the use of generic and shared accounts and ensure users can always be identified for their actions within ICT systems.

EXAMPLES OF EVIDENCE

- Clear definitions of user roles and their corresponding access rights.
- A central record (register or database) detailing all granted access rights, including user names, roles, access levels and dates of access changes.
- Approved access request forms supporting entries in the access rights register. Granting, withdrawals and changes of access should be appropriately documented and visible in the register and consistent with the process for granting and withdrawing access rights (Annex to the regulation, point 11.2.2). It is also important that archived backups are properly secured to prevent unauthorised access. It should be remembered that in the case of these copies, excessive permissions should be limited and controlled.
- Periodic access reviews meaning evidence of regular reviews of user access rights to ensure they remain appropriate over time.
- System logs showing all access rights management activities (creation, modification and deletion).
- Audit trail logs demonstrating access rights management, including timestamps, user IDs and actions performed.
- Records of incidents related to access rights management, including unauthorized access attempts and corrective actions.

([90]) Implementing a unique centralised database would require major interfacing work with systems that, in many cases, were not designed for it.

- Evidence of systems enforcing access controls, such as identity and access management (IAM) solutions.
- Reports from internal or external compliance audits verifying alignment with the access control policy.
- Results of physical inspections of access control systems and their use, if applicable.

11.2.3. The relevant entities shall review access rights at planned intervals and shall modify them based on organisational changes. The relevant entities shall document the results of the review including the necessary changes of access rights.

GUIDANCE

- Regularly review physical and logical access rights, taking into account:
  - users' access rights after termination or change of employment;
  - authorisations for privileged access rights.
- Review and update the inventory of the authentication and authorization systems regularly.
- Perform access control reviews of assets to verify that all privileges are authorised on a recurring schedule at least annually.

EXAMPLES OF EVIDENCE

- A central record (register or database) detailing all granted access rights, including user names, roles, access levels and dates of access changes.
- Approved access request forms supporting entries in the access rights register.
- Periodic access reviews meaning evidence of regular reviews of user access rights to ensure they remain appropriate over time.
- System logs showing all access rights management activities (creation, modification and deletion).
- Audit trail logs demonstrating access rights management, including timestamps, user IDs and actions performed.
- Records of incidents related to access rights management, including unauthorized access attempts and corrective actions.
- Reports from internal or external compliance audits verifying alignment with the access control policy.
- Physical inspection results of access control systems and their use, if applicable.
- Records of reviews and updates showing that access rights are reviewed regularly and updated as necessary.

TIPS

GUIDANCE

- Centralize access control for all assets through a directory service or single sign on (SSO) provider, where supported.
- Implement a segregation of duties matrix and ensure that it is updated dynamically by automating how changes are handled in response to role assignments or task changes (e.g. integration with access control, IAM or enterprise resource planning (ERP) systems).

EXAMPLES OF EVIDENCE

- Evidence of a centralized directory service or SSO provider to manage access control, supported by documentation, logs, audit reports and records.
- Segregation of duties matrix.

11.3 PRIVILEGED ACCOUNTS AND SYSTEM ADMINISTRATION ACCOUNTS

11.3.1. The relevant entities shall maintain policies for management of privileged accounts and system administration accounts as part of the access control policy referred to in point 11.1.

GUIDANCE

- Allocate privileged access rights to users as needed and, on an event-by-event basis in line with the access control policy referred to in point 11.1 of the Annex to the regulation (that is, only to individuals with the necessary authority to carry out activities that require privileged access and based on the minimum requirement for their functional roles).
- Identify users who need privileged access ([91]) to a network and information system (e.g. operating systems, database management systems and applications). This should include any privileged physical access to, e.g. cryptographic codes, keys or devices and in line with point 13.3 of the Annex to the regulation.
- Where appropriate, maintain an authorization process and a record of all allocated privileged access rights, consistent with the process for granting and revoking access rights (Annex to the regulation, point 11.2.2).

EXAMPLES OF EVIDENCE

- Clear policy on privileged account usage and access rules for privileged accounts.
- List of users with privileged access and what systems they can access.
- Documented approval records for granting privileged access.
- Logs or records of access reviews and revocations.
- Role-based access matrix showing who needs what access.

11.3.2. The policies referred to in point 11.3.1. shall:

(a) establish strong identification, authentication such as multi-factor authentication and authorisation procedures for privileged accounts and system administration accounts;

(b) set up specific accounts to be used for system administration operations exclusively, such as installation, configuration, management or maintenance;

(c) individualise and restrict system administration privileges to the highest extent possible,

(d) provide that system administration accounts are only used to connect to system administration systems.

GUIDANCE

- Introduce higher authentication requirements for privileged access rights, such as re-authentication or authentication step-up before using privileged access rights.
- Define and implement expiry requirements for privileged access rights, where appropriate.
- In the absence of a system that allows all uses to be attributed to an individual with certainty, establish specific rules to avoid the use of generic administration user IDs (e.g. ‘root’) and manage and protect the authentication information of such identities.
- Grant temporary privileged access only for the time necessary to implement approved changes or activities (e.g. for maintenance activities), rather than permanently granting privileged access rights.

[91] “Privileged access rights are access rights provided to an identity, a role or a process that allows the performance of activities that typical users or processes cannot perform. System administrator roles typically require privileged access rights.” ISO/IEC 27002, 8.2. Privileged access rights.

  - Consider the frequency of system administration operations: daily tasks (e.g. backups and email routing) versus weekly or monthly tasks (e.g. reviewing memory and disk space).
- Log all privileged access for audit purposes;
- Assign separate identities with privileged access rights to individual users, rather than sharing or linking identities. Group identities for easier management if needed.
- Use identities with privileged access rights exclusively for administrative tasks, not for day-to-day general tasks such as checking email or accessing the web. Where feasible ([92]), separate privileged identities should be assigned for administrative tasks.
- Ensure users are aware of their privileged access rights or when they are in privileged access mode, for example using specific user identities, user interface settings or equipment.

EXAMPLES OF EVIDENCE

- Measures for privileged access control and monitoring for privileged accounts, including granting and revoking privileged access rights.
- Access assignment records showing how access rights are initially granted, based on job roles and responsibilities.
- Clear definitions of user roles and the corresponding access rights associated with each role.
- Audit trail and monitoring logs that capture the use of access rights, including any unauthorized access attempts and actions taken in response.

11.3.3. The relevant entities shall review access rights of privileged accounts and system administration accounts at planned intervals and be modified based on organisational changes and shall document the results of the review, including the necessary changes of access rights.

GUIDANCE

- Verify whether the duties, roles, responsibilities and competences of system administrators still qualify them for working with privileged access rights.

EXAMPLES OF EVIDENCE

- Records of reviews and updates showing that access rights are reviewed regularly and updated as necessary.
- Periodic access reviews meaning evidence of regular reviews of user access rights to ensure they remain appropriate over time.
- Change management logs of changes to access rights, reflecting any alterations due to role changes or termination of employment.
- Compliance audits with reports from internal or external audits verifying that the management of access rights aligns with the policy and regulatory requirements.

([92]) In environments such as Microsoft 365 where enforcing separate identities may conflict with Conditional Access, device compliance or session controls, privileged users may use a single identity provided that some additional compensating measures are in place e.g. MFA, just-in-time access, session logging, context-aware controls (e.g. location, device compliance, app enforcement) etc.

11.4 ADMINISTRATION SYSTEMS

11.4.1. The relevant entities shall restrict and control the use of system administration systems in accordance with the access control policy referred to in point 11.1.

GUIDANCE

- Access to system administration systems must be strictly controlled in line with the access control policy. Only authorized personnel should be granted such access and all activity must be logged and regularly reviewed.
- Measures should be in place to detect unauthorized access and ensure accountability through audit trails and periodic security assessments.
- Access logs from system administration systems should be integrated into the entity's centralized log management or SIEM solution. Automated alerts must be configured to detect and notify of any suspicious or unauthorized access attempts, ensuring a timely response and ongoing compliance with security policies.
- The retention period for logs must be clearly defined based on business needs, legal requirements and network and information security objectives.
- Logs should capture relevant events necessary for security monitoring, incident detection and forensic analysis, such as access attempts, administrative actions and system changes.

EXAMPLES OF EVIDENCE

- Regularly maintained logs that track access to system administration systems ([93]).
- Audit reports from internal or external security audits that assess compliance with the policy.

11.4.2. For that purpose, the relevant entities shall:
(a) only use system administration systems for system administration purposes and not for any other operations;
(b) separate logically such systems from application software not used for system administrative purposes,
(c) protect access to system administration systems through authentication and encryption.

GUIDANCE

- Implement strict access controls to ensure that administrative systems are used exclusively for their intended purpose. For instance, only allow authorised personnel with specific roles (e.g. system administrators and IT staff) access to system administration systems.
- Physically or logically isolate administrative systems from other application servers, for example use network segmentation to create separate zones for system administration systems and other systems, such as application servers. If applicable, physically inspect server racks to ensure separation.
- Require strong authentication mechanisms such as MFA for accessing system administration systems.
- Encrypt communication channels (e.g. secure shell protocol, hypertext transfer protocol secure) to protect data in transit to and from system administration systems.
- Encrypt sensitive configuration files and credentials stored on system administration systems.

([93]) Administration systems refer to the tools and processes used to manage, monitor and maintain the hardware, software and network components of an entity's IT infrastructure. Typical key functions of administration systems include (indicative, non-exhaustive list): system monitoring, configuration management, security management, user management and back-up and recovery.

- Ensure that application protocols are securely implemented. In addition, verify that any SSO or federation protocols are correctly implemented and conform to their specifications.

EXAMPLES OF EVIDENCE

- Regularly maintained logs that track access to system administration systems.
- Network segmentation documentation indicating how system administration systems are logically or physically separated from other systems.
- Documented authentication methods used to secure access to administration systems.
- Information on encryption protocols applied to protect data transmitted to and from system administration systems.

TIPS

GUIDANCE

- Consider using a centralized privileged access management (PAM) solution.
- Consider using a cloud access security broker (CASB) to enhance the visibility of, control over and the security of cloud service usage.
- Regularly audit system logs to monitor usage patterns and identify any unauthorised activities.
- Train personnel in the proper use of system administration systems.

EXAMPLES OF EVIDENCE

- Regularly maintained logs that track access to administration systems.
- Incident response records of any incidents related to system administration system misuse or unauthorized access.
- User training records meaning evidence that personnel have been trained in the proper use of system administration systems, for example training materials, attendance records or completion certificates.

11.5 IDENTIFICATION

11.5.1. The relevant entities shall manage the full life cycle of identities of network and information systems and their users.

GUIDANCE

- Establish and maintain an inventory of all identities managed in the entity.
  - The inventory should include both user and privileged or system administrator identities. The inventory should contain, as a minimum, the person’s name, username, start/stop dates and the level of privileges for each identity.
  - The inventory should also include all service identities and have these identity records as a minimum including department owner, review date, purpose and the level of privileges for each service identity.

EXAMPLES OF EVIDENCE

- Documented policy or procedure related to identity management, if available.
- Reports from internal or external audits verifying that the management of identities aligns with the policy and regulatory requirements.

11.5.2. For that purpose, the relevant entities shall:

(a) set up unique identities for network and information systems and their users;

(b) link the identity of users to a single person;

(c) ensure oversight of identities of network and information systems;

(d) apply logging to the management of identities.

GUIDANCE

- Consider that providing or revoking access to assets is usually a multi-step procedure:
  - confirming the business requirements for an identity to be established;
  - verifying the identity of an entity before allocating them a logical identity;
  - establishing an identity;
  - configuring and activating the identity, which also includes configuration and initial setup of related authentication services; and
  - providing or revoking the identity's specific access rights, based on appropriate authorization or entitlement decisions (section 11.2).
- Make sure that identities assigned to network and information systems (non-human users) are subject to appropriately segregated approval and independent ongoing oversight.
- Apply logging to the management of identities in cooperation with human resource security (section 10.1) where possible.

EXAMPLES OF EVIDENCE

- Identity records, for example user profiles with unique identifiers (e.g. usernames and employee IDs) and evidence of linking these identities to specific individuals (e.g. HR records).
- Logs of reviews or approvals for identities for network and information systems and their users.
- Logs or reports related to identity management.
- Evidence of the systems in place that enforce access control, such as IAM solutions.

11.5.3. The relevant entities shall only permit identities assigned to multiple persons, such as shared identities, where they are necessary for business or operational reasons and are subject to an explicit approval process and documentation. The relevant entities shall take identities assigned to multiple persons into account in the cybersecurity risk management framework referred to in point 2.1.

GUIDANCE

- Shared identities should be avoided unless strictly necessary for business or operational reasons ([94]). In such cases, their use must be formally justified, explicitly approved and properly documented. Examples of technical, procedural and governance controls to enhance their protection include (indicative, non-exhaustive list):
  - MFA enforcement;
  - Least privilege concept enforcement;
  - Time-bound or just-in-time access;

([94]) Wherever possible, the organization shall implement Role-Based Access Control (RBAC) to assign privileges to individual identities based on defined business or operational functions. RBAC must be used to avoid the creation of shared accounts unless a technical or operational constraint makes their use unavoidable.

- Checking out the shared credentials through a tool which logs who accessed the identity and when. If check-out is not possible, consider using privileged session recording or proxy-based access auditing;
- Session attribution techniques to link shared identity use back to individual users;
- Logging;
- Credential vaulting with auto-rotation;
- Prohibition of storing shared credentials in personal files, emails or messaging platforms;
- Network segmentation so that shared account use is limited to isolated network segments or virtual environments; and
- Mandatory training on acceptable use and accountability.

- These identities should be clearly recorded in the cybersecurity risk management framework, with appropriate controls in place to mitigate associated risks, including enhanced monitoring and accountability measures.

EXAMPLES OF EVIDENCE

- Approval records for exceptions.

11.5.4. The relevant entities shall regularly review the identities for network and information systems and their users and, if no longer needed, deactivate them without delay.

GUIDANCE

- Verify that all active identities are reviewed. This can be done on a recurring schedule, as a minimum quarterly, or more frequently. However, for micro-sized entities, this can be done annually.
- Disable or remove, in a timely fashion, identities that they are no longer required, for example delete or disable any dormant identities after a predefined period of days of inactivity, where supported.

EXAMPLES OF EVIDENCE

- Records of reviews and updates showing that identities are reviewed regularly and updated as necessary.
- Records of changes to identities, reflecting any alterations due to role changes or termination of employment or inactivity.

TIPS

GUIDANCE

- Centralize identity management through a directory or identity service.
- Where appropriate, define different levels of identification required based on role, use or need.

EXAMPLES OF EVIDENCE

- Evidence of the systems in place, such as IAM solutions.

11.6 AUTHENTICATION

11.6.1. The relevant entities shall implement secure authentication procedures and technologies based on access restrictions and the policy on access control.

GUIDANCE

- Authentication technologies are methods used to verify the identity of users, devices or systems before granting access to resources. Here are some common authentication technologies (indicative, non-exhaustive list):
  - password-based authentication,
  - passkeys,
  - two-factor authentication,
  - MFA ([95]),
  - biometric authentication,
  - token-based authentication, such as a one-time passcode (OTP),
  - smart cards,
  - Fast Identity Online 2 security keys,
  - certificate-based authentication,
  - SSO,
  - OpenID Connect.

EXAMPLES OF EVIDENCE

- Access control policy documents outlining secure authentication procedures and technologies.
- Logs from authentication systems showing successful and failed authentication attempts, which demonstrate secure implementation.
- Evidence of the systems in place that enforce access controls, such as IAM solutions.
- Internal or external audit reports verifying the implementation of secure authentication procedures aligned with the access control policy.
- Documentation that shows the use of secure authentication and authorization protocols and demonstrates that these have been tested to confirm that they are implemented in a secure fashion.

11.6.2. For that purpose, the relevant entities shall:

(a) ensure the strength of authentication is appropriate to the classification of the asset to be accessed;

(b) control the allocation to users and management of secret authentication information by a process that ensures the confidentiality of the information, including advising personnel on appropriate handling of authentication information;

(c) require the change of authentication credentials initially, at predefined intervals and upon suspicion that the credentials were compromised;

(d) require the reset of authentication credentials and the blocking of users after a predefined number of unsuccessful log-in attempts;

(e) terminate inactive sessions after a predefined period of inactivity; and

(f) require separate credentials to access privileged access or administrative accounts.

([95]) When implementing, the entity should take into account MFA fatigue, which can occur when users are overwhelmed when they receive numerous authentication prompts. Consider techniques to mitigate this, such as adaptive MFA, passkeys, MFA combined with SSO and short session timeouts.

GUIDANCE

- Use unique authentication credentials for all the entity's assets. Best-practice implementation includes, as a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.
- Consider that the allocation and management process for authentication information should ensure that:
  - passwords or PINs generated automatically during enrolment processes as temporary secret authentication information are non-guessable and unique for each user; and that users are required to change them after the first use;
  - procedures are established to verify the identity of a user prior to providing new, replacement or temporary authentication information;
  - authentication information, including temporary authentication information, is transmitted to users in a secure manner (e.g. via an authenticated and protected channel), and the use of unprotected (clear text) electronic mail messages is avoided;
  - users acknowledge receipt of authentication information;
  - default authentication information as predefined or provided by suppliers is changed immediately following installation of systems or software;
  - records of significant events concerning allocation and management of authentication information are kept and their confidentiality granted, and that the record keeping method is approved (e.g. using an approved password vault tool).
- When passwords are used as authentication information, the password management system should:
  - allow users to select and change their own passwords and include a confirmation procedure to address input errors;
  - enforce strong passwords ([96]);
  - force users to change their passwords at first login, if relevant;
  - enforce password changes as necessary, for example after a security incident or upon termination or change of employment when a user has known passwords for identities that remain active (e.g. shared identities);
  - prevent the use of commonly used passwords, and compromised combinations of usernames and password from hacked systems;
  - not display passwords on the screen when they are being entered; and
  - store and transmit passwords in protected form.
- The use of phishing-resistant MFA is recommended. Below is a list of currently available solutions ordered from strongest to weakest.
  - 'Strong':
    - phishing-resistant:
      - no shared secrets, not vulnerable to attacker-in-the-middle;
      - protected cryptographic private key that can be securely registered to:
        - a domain, in accordance with Fast Identity Online (FIDO) and W3C WebAuthn standards;

([96]) Password complexity can be a good cybersecurity practice, but it is not the only factor to consider. Recent guidelines, such as those from NIST, emphasise password length over complexity; see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.2pd.pdf, line 725.

        - a trust provider, following public key infrastructure and International Telecommunication Union X.509 standards.
    - 'Medium' MFA, for example:
        - push notification, number matching or application based.
    - 'Last resort' MFA, for example:
        - text message or email OTP.
- Perform password encryption and hashing in accordance with approved cryptographic techniques for passwords (section 9.2).
- Generate an alert when a potential attempted or successful breach of login controls is detected.

EXAMPLES OF EVIDENCE

- Logs or reports related to authentication.
- Compliance audits from internal or external audits verifying that the management of identities aligns with the policy and regulatory requirements.
- Documentation showing that the identities are reviewed regularly and updated as necessary.
- Records of changes to identities, reflecting any alterations due to role changes or termination of employment.

11.6.3. The relevant entities shall to the extent feasible use state-of-the-art authentication methods, in accordance with the associated assessed risk and the classification of the asset to be accessed and unique authentication information.

GUIDANCE

- Adjust authentication methods based on the associated assessed risk. For example, require additional authentication for high-risk transactions or access to assets of higher criticality.
- Use more stringent authentication methods for assets of higher criticality.
- Ensure each user has unique credentials. Avoid shared accounts and implement strict policies for credential management.

EXAMPLES OF EVIDENCE

- Access control policy documents outlining secure authentication procedures and technologies.

11.6.4. The relevant entities shall regularly review the authentication procedures and technologies at planned intervals.

GUIDANCE

- Conduct periodic audits of authentication procedures and technologies to ensure they remain up to date, where appropriate and effective against emerging threats.
- Stay up to date on advancements in authentication technology and integrate new methods as they become available.

EXAMPLES OF EVIDENCE

- Internal or external audit reports detailing the results of periodic audits of authentication procedures and technologies.
- Logs showing the implementation of new authentication technologies and methods as they become available

TIPS

GUIDANCE

- Advise any user with access to or using authentication information to comply with the following.
  - Secret authentication information, such as passwords, is kept confidential. Personal secret authentication information is not to be shared with anyone. Secret authentication information used in the context of identities linked to multiple users or linked to non-personal entities is solely shared with authorised persons.
  - Affected or compromised authentication information is changed immediately upon notification of or any other indication of a compromise.
  - When passwords are used as authentication information, strong passwords according to best practice recommendations are selected. For example, passwords are not based on anything somebody else can easily guess or obtain using person-related information (e.g. names, telephone numbers and dates of birth); passwords are not based on dictionary words or combinations thereof; use easy to remember passphrases and try to include alphanumerical and special characters; passwords should have a minimum length.
  - The same credentials are not used across different network and information systems.
  - The obligation to follow these rules is also included in the terms and conditions of employment.

EXAMPLES OF EVIDENCE

- Documentation of training sessions for employees on secure authentication practices and technologies.
- Records of awareness programmes or communications to employees about the importance of secure authentication.

11.7 MULTI-FACTOR AUTHENTICATION

11.7.1. The relevant entities shall ensure that users are authenticated by multiple authentication factors or continuous authentication mechanisms for accessing the entities' network and information systems, where appropriate, in accordance with the classification of the asset to be accessed.

GUIDANCE

- Select appropriate MFA ([97]) methods and continuous authentication mechanisms based on the entity's security needs and depending on the classification of the asset. It is also good practice to consider user convenience when selecting and implementing a solution:
  - test-message-based OTP: simple but less secure due to risks such as SIM swapping;
  - authenticator apps: generate time-based OTPs;
  - push notifications: send an approval request to a user's device;
  - hardware tokens: for example physical devices generating OTPs, smart cards;
  - passkeys;
  - Fast Identity Online 2 security keys;
  - biometrics: fingerprints, facial recognition, etc.

([97]) Some types of MFA are vulnerable to phishing attacks, and the relevant entities should select MFA that can stand up to these attacks. For more information (indicative), see https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf and https://doubleoctopus.com/blog/general/phishing-resistant-mfa-guide/.

- Consider continuous authentication ([98]) for avoiding specific threats such as session hijacking, credential theft and insider threats.

EXAMPLES OF EVIDENCE

- Logs showing MFA being used to access network and information systems.
- Configuration of authentication solutions implementing MFA.
- Access control policy outlining how different MFA methods are assigned, including whether phishing-resistant MFA is used.

11.7.2. The relevant entities shall ensure that the strength of authentication is appropriate for the classification of the asset to be accessed.

GUIDANCE

- Determine which network and information systems require the use of MFA protection based on the classification of the asset to be accessed. Wherever possible, use phishing-resistant MFA.
- Analyse user roles and the level of access required by each role to determine appropriate MFA methods.
- Consider MFA, in particular when accessing systems from a remote location, accessing system administration systems, access to sensitive information, etc.
- Enforce MFA on internet-facing systems, such as email, remote desktop and VPNs ([99]).
- Define when and how MFA is required (e.g. every login, once per session or for high-risk actions).

EXAMPLES OF EVIDENCE

- Documentation detailing the classification of assets and the associated requirement for MFA protection.
- Risk assessment results justifying the need for MFA on certain network and information systems.
- List of user roles, associated access rights and the analysis conducted to determine appropriate MFA methods.
- Configuration files and logs showing MFA enabled on specific network and information systems.
- Settings from authentication systems reflecting the defined MFA requirements.
- Logs from authentication systems showing enforcement of these MFA requirements.

TIPS

GUIDANCE

- Integrate MFA with SSO solutions for seamless access. Wherever possible, use phishing-resistant MFA.
- Implement secure fallback methods for users who lose access to their MFA methods.
- Educate users about the importance of MFA and how to use it.
- Regularly monitor MFA logs for suspicious activity.
- Keep the MFA system and associated devices updated.

([98]) Unlike traditional authentication, which verifies users only at the time of login, continuous authentication dynamically assesses developing risk factors such as location, device status and behavioural patterns throughout the session. Different authentication methods (see section 11.6.1) can be combined during continuous authentication.

([99]) CyberFundamentals, PR.AC-3, Centre for Cyber Security Belgium, https://atwork.safeonweb.be/sites/default/files/2024-12/cyfun_basic_v2023-03-01_e_update_2024.pdf.

- Combine MFA with other techniques to require additional factors under specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.
- Evaluate and choose an MFA provider that fits the entity's requirements:
  - ease of integration: ensure the MFA solution integrates well with the existing systems;
  - user experience: aim for a balance between security and user convenience;
  - scalability: choose a solution that can grow with the entity;
  - support and reliability: ensure the provider offers robust support and high reliability.
- Pilot test the MFA solution with a small group of users.
- Ensure that MFA implementation meets legal requirements (e.g. the GDPR).

EXAMPLES OF EVIDENCE

- Manuals, configuration files or screenshots demonstrating the successful integration of MFA with an SSO provider.
- Records of training sessions, attendance lists and training materials provided to users about the importance and usage of MFA.
- Regularly generated reports from MFA systems showing log monitoring activities and any suspicious activities detected.
- Configuration files showing the implementation of additional authentication factors based on predefined rules.

ASSET MANAGEMENT

12. ASSET MANAGEMENT

12.1 ASSET CLASSIFICATION

12.1.1. For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall lay down classification levels of all assets, including information, in scope of their network and information systems for the level of protection required.

GUIDANCE

- Create and document classification levels for the assets, including conventions for classification.

EXAMPLES OF EVIDENCE

- Documented classification levels for the assets.

12.1.2. For the purpose of point 12.1.1., the relevant entities shall:
(a) lay down a system of classification levels for assets;
(b) associate all assets with a classification level, based on confidentiality, integrity, authenticity and availability requirements, to indicate the protection required according to their sensitivity, criticality, risk and business value;
(c) align the availability requirements of the assets with the delivery and recovery objectives set out in their business continuity and disaster recovery plans.

GUIDANCE

- Ensure that classifications and associated protective measures for assets consider business needs, including:
  - sharing or restricting information;
  - protecting the integrity and authenticity of information;
  - ensuring availability ([100]); and
  - complying with legal requirements concerning the confidentiality, integrity or availability of the information.
- Define and communicate a classification for sensitive information, such as (indicative example):
  - public - freely accessible to all, even externally;
  - internal - accessible only to members of the entity;
  - confidential - accessible only to those whose duties require access.
- Use classifications derived from national law, international agreements or internationally accepted strategies for sharing information, such as the traffic light protocol.
- Align the classification with the access control policy (section 11.1).
- Classify assets in accordance with the identified classification levels.
- Classify assets other than information in accordance with the classification of the information they store, process, handle or protect.

([100]) For example, the entity could assess the direct replacement cost associated with an asset and, where possible, the known indirect cost of total loss.

EXAMPLES OF EVIDENCE

- The latest, updated record of the entity's assets and their classification based on the identified classification levels.

12.1.3. The relevant entities shall conduct periodic reviews of the classification levels of assets and update them, where appropriate.

GUIDANCE

- Define criteria for reviewing the classification over time.
- Review the classification at least annually, taking into account:
  - regulatory changes; and
  - changes in the value, sensitivity and criticality of the assets throughout their life cycle.

EXAMPLES OF EVIDENCE

- Documentation showing the schedule for reviews.
- Records of the most recent review and logs detailing changes made during the last review, including reclassifications and the addition/removal of assets.

TIPS

GUIDANCE

- Ensure that owners of the assets are responsible for their classification.
- Communicate to personnel the classification of assets and associated protection requirements.

EXAMPLES OF EVIDENCE

- Personnel knowing classification levels and protection requirements for each level.

12.2 HANDLING OF ASSETS

12.2.1. The relevant entities shall establish, implement and apply a policy for the proper handling of assets, including information, in accordance with their network and information security policy and shall communicate the policy on proper handling of assets to anyone who uses or handles assets.

GUIDANCE

- Ensure that employees, direct suppliers, service providers and any other third parties who use or handle the entity's assets ([101]) are aware of the policy.
- Consider mobile devices, such as smartphones and tablets, and determine a strategy for mobile device management, including Bring-Your-Own-Device (BYOD) ([102]).

EXAMPLES OF EVIDENCE

- Policy on the proper handling of assets.

([101]) Vehicles that can store data locally on the vehicle and/or share data externally by means of telematics are included.
([102]) BSI, 'SYS.3.2.1 Mobile Device Management, IT-Grundschutz-Compendium', English version, 1 February 2022, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.html.
NIST Special Publication 800-46, 'Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security', https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf.

- User manuals or instructions provided to employees, direct suppliers, service providers and any other third parties who use or handles the entity's assets.
- Documentation showing that employees have completed training sessions on the asset handling policy.
- Forms or electronic records that employees, direct suppliers, service providers and third parties have signed to acknowledge they have read and understood the policy.

12.2.2. The policy shall:
(a) cover the entire life cycle of the assets, including acquisition, use, storage, transportation and disposal;
(b) provide instructions on the safe use, safe storage, safe transport and the irretrievable deletion and destruction of the assets;
(c) provide that the transfer shall take place in a secure manner, in accordance with the type of asset or information to be transferred.

GUIDANCE

- Identify, document and implement a policy for handling assets ([103]) throughout their life cycle (acquisition, use, storage, transportation and disposal).
- Ensure that the policy includes at least safe storage, safe transport; and irretrievable deletion and destruction. For example:
  - create user manuals and training materials on the correct and secure use of assets;
  - establish guidelines for secure storage, taking into account backup management (section 4.2);
  - define protocols for secure transfer, including consider secure migration processes, when transferring data to a cloud service;
  - outline methods for data wiping and physical destruction, ensuring complete and irretrievable deletion.
- Ensure that the policy covers the proper usage of all in-scope assets, both on-premises and off-premises (e.g. mobile devices, data in the cloud, transient data ([104]) or sensitive information).
- Ensure that assets may be transferred to external premises only after approval by authorized management bodies, in accordance with the policy.
- Link the asset handling policy with the asset classification by providing handling details for each classification level.

EXAMPLES OF EVIDENCE

- Documented policy for handling assets.
- User access lists, access request forms and approval records.
- Incident reports related to asset handling (e.g. loss, theft or damage).

12.2.3. The relevant entities shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations or risks occur.

GUIDANCE

- Review and update the policy for asset handling at least annually.

([103]) Vehicles that can store data locally on the vehicle and/or share data externally by means of telematics are included.
([104]) Data that moves between systems, users, or devices, often temporarily or for processing purposes.

EXAMPLES OF EVIDENCE

- Up-to date policy for asset handling
- Records of reviews or history of changes.

12.3 REMOVABLE MEDIA POLICY

12.3.1. The relevant entities shall establish, implement and apply a policy on the management of removable storage media and communicate it to their employees and third parties who handle removable storage media at the relevant entities' premises or other locations where the removable media is connected to the relevant entities' network and information systems.

GUIDANCE

- Define, document and implement a policy on the management of removable media ([105]).
- Communicate the policy to employees and third parties who handle removable storage media to ensure that they are aware of the policy.

EXAMPLES OF EVIDENCE

- Documented policy on the management of removable media, including at least the items in point 12.3.2 of the Annex to the regulation.
- User manuals or instructions provided to employees and third parties concerning the correct usage of the removable media.
- Documentation showing that employees and third parties have completed training sessions on the policy or forms or electronic records that employees and third parties have signed to acknowledge they have read and understood the policy.
- Evidence of ongoing awareness campaigns, such as posters, emails or intranet posts, reminding employees about the risks and policies associated with removable media.

12.3.2. The policy shall:

(a) provide for a technical prohibition of the connection of removable media unless there is an organisational reason for their use;

(b) provide for disabling self-execution from such media and scanning the media for malicious code before they are used on the relevant entities' systems;

(c) provide measures for controlling and protecting portable storage devices containing data while in transit and in storage;

(d) where appropriate, provide measures for the use of cryptographic techniques to protect data on removable storage media.

GUIDANCE

- Align the policy with the asset classification (section 12.1) and include at least the following:
    - definitions and scope of removable media,
    - authorization requirements,
    - usage guidelines,

([105]) Including 'bring your own device', if personal devices are used to store corporate data. Vehicles that can store data locally on a vehicle and/or share data externally by means of telematics are also included.

  - measures for control and protection of removable media while in storage and in transit;,
  - techniques to protect information on removable storage media and
  - incident response procedures for lost or compromised media.
- Configure network and information systems to disable the autorun feature for all removable media, to prevent the automatic execution of potentially malicious software.
- If connection of removable media is not prohibited for an organisational (business) reason, removable media should be scanned for malicious code, where appropriate, with up-to-date software against malicious code before being connected to the entity's network and information systems and/or in real time.
- Encrypt sensitive data stored on removable media using strong cryptographic algorithms to protect against unauthorized access
- Use encryption to protect data stored on portable storage devices, ensuring that unauthorized users cannot access the data if the device is lost or stolen.
- Implement physical security measures, where appropriate, such as secure storage locations and tracking logs for portable storage devices.

EXAMPLES OF EVIDENCE

- Configuration settings of endpoint protection software, if any.
- Audit logs that track the use of removable media, including insertion, removal and data transfer activities.
- Reports of incidents involving removable media, if any.

12.3.3. The relevant entities shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations or risks occur.

GUIDANCE

- Regularly monitor and audit the use of removable media to ensure compliance with the policy.

EXAMPLES OF EVIDENCE

- Up-to date removable media policy.
- Records of reviews or history of changes.

12.4 ASSET INVENTORY

12.4.1. The relevant entities shall develop and maintain a complete, accurate, up-to-date and consistent inventory of their assets. They shall record changes to the entries in the inventory in a traceable manner.

GUIDANCE

- Ensure that all assets, including hardware, software, data and services, are listed in the inventory.
- Regularly verify the accuracy of the inventory entries.
- Update the inventory promptly to reflect any changes, such as new assets, decommissioned assets or changes in asset status (section 6.4)
- Use standardised naming conventions and categorization methods to maintain consistency across the inventory.
- Make sure that inventory entries contain the data in the guidance below (sampling).
- Implement validation rules within the inventory to ensure data entered is complete and consistent.

EXAMPLES OF EVIDENCE

- Documentation for the inventory of assets
- Up to date inventory of assets
- Records of reviews or history of changes.
- Records of key metrics tracked, such as the number of assets, types of assets, compliance with inventory policies and the timeliness of updates.

12.4.2. The granularity of the inventory of the assets shall be at a level appropriate for the needs of the relevant entities. The inventory shall include the following:
(a) the list of operations and services and their description,
(b) the list of network and information systems and other associated assets supporting the relevant entities' operations and services.

GUIDANCE

- Consider adding one or more of the following to the inventory (indicative, non-exhaustive list):
  - asset unique ID,
  - asset type, for example software including virtual machines (version), hardware (operating system / firmware), services, supporting utilities, facilities, heating, ventilation and air conditioning (HVAC) systems, personnel and physical records,
  - asset owner and contact information,
  - operational unit responsible for the asset, either internal department name or external provider name ([106]),
  - asset description,
  - asset location,
  - date of asset's last update/patch,
  - asset classification consistent with the risk assessment,
  - type of information and its classification processed in the basset,
  - asset end of life, where applicable,
  - relation to other assets and
  - logging requirements.

EXAMPLES OF EVIDENCE

- Configuration of the asset inventory tool, if any.

12.4.3. The relevant entities shall regularly review and update the inventory and their assets and document the history of changes.

GUIDANCE

- Conduct regular reviews to verify the accuracy and completeness of the inventory.
- Maintain history of changes.

([106]) In the case of external provider(s), a reference to the SLA covering this relation will also be useful.

EXAMPLES OF EVIDENCE

- Up-to-date inventory of assets including history of changes.
- Regular reports generated on inventory status, changes and audit findings.

TIPS

GUIDANCE

- Use tools that support the comprehensive tracking and management of assets.
- Ideally, consider the use of tools for automated discovery and asset tracking to continuously discover, categorize, and monitor both on-premises and cloud assets, ensuring comprehensive, up-to-date visibility and security. Alternatively, consider manual update procedures.
- Configure the chosen tool to capture the defined attributes and categories, ensuring it supports relevant functionalities such as tagging, searching and reporting.
- Set up automated alerts for missing or incomplete data, discrepancies and anomalies detected in the inventory.

EXAMPLES OF EVIDENCE

- Configuration settings of the asset management tool.

12.5 DEPOSIT, RETURN OR DELETION OF ASSETS UPON TERMINATION OF EMPLOYMENT

The relevant entities shall establish, implement and apply procedures which ensure that their assets which are under custody of personnel are deposited, returned or deleted upon termination of employment and shall document the deposit, return and deletion of those assets. Where the deposit, return or deletion of assets is not possible, the relevant entities shall ensure that the assets can no longer access the relevant entities' network and information systems in accordance with point 12.2.2.

GUIDANCE

- Define procedures to ensure that assets are deposited, returned or irrevocably deleted on termination of employment or contractual relationships.
- Make sure that the procedures clearly identify all assets to be returned, according to the asset inventory (Annex to the regulation, point 12.4.1), which can include (indicative, non-exhaustive list):
  - user endpoint devices, e.g. computers, tablets and phones etc and/or portable storage devices, including vehicles, that can store data locally on the vehicle and/or share data externally by means of telematics. Identify where the user process, transfer or store entity data to determine the scope of user endpoint devices;
  - specialised equipment;
  - authentication hardware (e.g. access cards, mechanical keys, physical tokens and smart cards);
  - physical copies of information.

EXAMPLES OF EVIDENCE

- Documented procedures for the timely return of assets upon termination of employment.
- Logs or records indicating that data on returned assets was deleted according to the procedures.

- Completed exit checklist forms that include asset return and data deletion steps, signed by the departing employee and relevant supervisors.

TIPS

GUIDANCE

- In cases where employees (and other third parties) use their own personal equipment, follow procedures to ensure that all relevant information is traced and transferred to the entity and securely deleted from the equipment.
- Keep a record of the implementation of the policy (list of employees who have left or contractors whose contracts have ended and list of the assets they returned, including return date).
- Make sure that relevant terms are part of the employment or service contract.
- Communicate the procedures to employees during the induction process and during the exit process.
- Check that there is an employee exit interview process and the return of the assets is linked with it.
- Where the deposit, return or deletion of assets is not possible (indicative, non-exhaustive list):
  - ensure that any credentials associated with the assets are revoked or disabled;
  - isolate the assets by placing them in a separate network segment;
  - use access control lists to restrict access to and from the isolated assets;
  - ensure that only authorised personnel can interact with these assets;
  - configure firewalls to block any traffic to and from the isolated assets;
  - physically or logically disable the network interfaces of the assets;
  - continuously monitor the isolated assets and log any access attempts.

EXAMPLES OF EVIDENCE

- Personnel aware of the procedures.
- Communication materials, such as emails or intranet posts, that remind employees of their obligations upon termination.
- Statements confirming that data was irrevocably deleted, especially for external employees or contractors.
- Documentation of the termination process, including coordination between HR and IT departments.
- Sample checks of lists of employees/contractors and the assets they were assigned and those they returned.

ENVIRONMENTAL AND PHYSICAL SECURITY

13. ENVIRONMENTAL AND PHYSICAL SECURITY

13.1 SUPPORTING UTILITIES

13.1.1. For the purpose of Article 21(2)(c) of Directive (EU) 2022/2555, the relevant entities shall prevent loss, damage or compromise of network and information systems or interruption to their operations due to the failure and disruption of supporting utilities.

GUIDANCE

- Consider supporting utilities, where relevant ([107]), that ensure the continuous operation of network and information systems, such as (indicative, non-exhaustive list):
    - power supply – electricity to keep systems running;
    - water for cooling and other operational needs;
    - gas for heating or backup power generation;
    - HVAC to maintain optimal operating conditions;
    - telecommunications – internet and network connectivity.
- Include the potential failure and disruption of supporting utilities in the risk assessment.

EXAMPLES OF EVIDENCE

- List of supporting utilities and associated risk assessment results.
- Measures to protect against the failure and disruption of supporting utilities.

13.1.2. For that purpose, the relevant entities shall, where appropriate:
(a) protect facilities from power failures and other disruptions caused by failures in supporting utilities such as electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning;
(b) consider the use of redundancy in utilities services;
(c) protect utility services for electricity and telecommunications, which transport data or supply network and information systems, against interception and damage;
(d) monitor the utility services referred to in point (c) and report to the competent internal or external personnel events outside the minimum and maximum control thresholds referred to in point 13.2.2(b) affecting the utility services;
(e) conclude contracts for the emergency supply with corresponding services, such as for the fuel for emergency power supply;
(f) ensure continuous effectiveness, monitor, maintain and test the supply of the network and information systems necessary for the operation of the service offered, in particular the electricity, temperature and humidity control, telecommunications and Internet connection.

([107]) In cases where an entity operates with a fully remote workforce and does not maintain any on-premises servers or infrastructure, the requirement for supporting utility services at a centralized location may be rendered unnecessary. Remote work inherently introduces geographical and infrastructural diversification, thereby reducing the overall utility-related risk. By distributing operations across various locations, the organization benefits from a decentralized utility dependency, which enhances resilience against localized disruptions.

GUIDANCE

- Consider the availability of supporting utilities in the business continuity plan (section 4.1).
- Consider the availability of supporting utilities, when implementing backup management (section 4.2).
- Consider implementing measures for the protection of supporting utilities, such as (indicative, non-exhaustive list):
  - active/passive cooling;
  - automatic restart after power interruption;
  - battery backup power;
  - diesel generators;
  - backup fuel;
  - uninterruptable power supply, hot standby power generators;
  - sufficient fuel delivery SLA;
  - delivery companies;
  - redundant cooling;
  - spare parts for components of network and information systems; and
  - power backup systems.

EXAMPLES OF EVIDENCE

- Description of different types of supporting utilities.
- Measures to protect against the failure and disruption of supporting utilities.

13.1.3. The relevant entities shall test, review and, where appropriate, update the protection measures on a regular basis or following significant incidents or significant changes to operations or risks.

GUIDANCE

- Conduct routine tests of protection measures.
- Set up periodic reviews to evaluate the effectiveness of current protection measures.

EXAMPLES OF EVIDENCE

- Updated measures to protect against the failure and disruption of supporting utilities, review comments and/or change logs.
- Evidence that the measures that protect supporting utilities against failures and disruptions are deployed and regularly tested.

TIPS

GUIDANCE

- Include a simulated total power failure in the verification of the testing procedure for power generators.
- Make employees aware of dependencies on supporting utilities.
- Train staff in how to respond effectively to failures and disruptions of supporting utilities.
- Set up monitoring systems to detect utility failures or disruptions.

EXAMPLES OF EVIDENCE

- Records of internal communications, emails or newsletters highlighting the importance of supporting utilities and their impact on operations.

- Logs demonstrating detection and recording of any utility failures or disruptions.

13.2 PROTECTION AGAINST PHYSICAL AND ENVIRONMENTAL THREATS

13.2.1. For the purpose of Article 21(2)(e) of Directive (EU) 2022/2555, the relevant entities shall prevent or reduce the consequences of events originating from physical and environmental threats, such as natural disasters and other intentional or unintentional threats, based on the results of the risk assessment carried out pursuant to point 2.1.

GUIDANCE

- Consider risks associated with current and forecasted physical and environmental threats to the network and information systems, where relevant ([108]).
  - Include in the assessment the (physical) locations of the entity's facilities.
- Based on the results of the risk assessment determine the assets that need to be protected from physical and environmental threats.

EXAMPLES OF EVIDENCE

- Risk assessment report that includes:
  - identification and evaluation of physical locations, such as data centres, offices and server rooms,
  - analysis of potential physical and environmental threats and
  - mapping of critical assets to physical locations.

13.2.2. For that purpose, the relevant entities shall, where appropriate:

(a) design and implement protection measures against physical and environmental threats;

(b) determine minimum and maximum control thresholds for physical and environmental threats;

(c) monitor environmental parameters and report to the competent internal or external personnel events outside the minimum and maximum control thresholds referred to in point (b).

GUIDANCE

- Implement measures against physical and environmental threats. Parameters to consider are (indicative, non-exhaustive list):
  - purpose and scope;
  - network and information systems in scope;
  - description of facilities;
  - roles and responsibilities;
  - management commitment;
  - coordination among organisational units;
  - compliance with national and EU law, including personal data protection.

([108]) Where a company operates with a fully remote workforce and lacks centralized on-premises infrastructure, traditional physical and environmental threat protections at a single location may be less critical. The distributed nature of remote work inherently provides resilience by diversifying exposure to localized physical and environmental risks. Consequently organizations should focus on ensuring that remote employees' home work environments meet minimum security and safety standards and consider leveraging cloud service providers' robust physical security controls. This distributed operational model reduces dependency on any single physical site, thereby mitigating the impact of localized environmental or physical incidents.

- Consider potential physical and environmental threats relevant to the context, location and operational environment. The following list offers examples (indicative and non-exhaustive) to support risk-based planning:
  - fire, flood or natural events (e.g. earthquakes, storms),
  - public disturbances or unauthorized access, theft or vandalism,
  - hazardous material incidents (e.g. chemical spills),
  - long-term environmental changes (e.g. climate trends, air quality).
- Consider measures against physical and environmental threats such as (indicative, non-exhaustive list):
  - physical access control measures (e.g. IDs, badges, logs; visitor management system and physical barriers);
  - surveillance systems (e.g. CCTV, entry points, exits, locking mechanisms and security personnel);
  - climate control (e.g. temperature and humidity controls and HVAC systems);
  - fire prevention and response measures (e.g. fire alarms, smoke detectors, sprinkler systems and fire extinguishers);
- Consider enhanced (maximum) measures to be activated during heightened threat levels or specific scenarios. Examples of such measures include (indicative, non-exhaustive list):
  - Increased security personnel, advanced biometric access controls and lockdown procedures.
  - Enhanced monitoring systems, redundant power supplies and advanced environmental sensors.

EXAMPLES OF EVIDENCE

- Detailed documentation showing the design and implementation of measures against physical and environmental threats.
- Reports outlining the defined minimum and maximum control thresholds for various threats.
- Logs from environmental monitoring systems showing continuous tracking of parameters, such as temperature, humidity and security breaches.
- Records of incidents where parameters fell outside the defined thresholds, including the actions taken and notifications sent to relevant personnel.

13.2.3. The relevant entities shall test, review and, where appropriate, update the protection measures against physical and environmental threats on a regular basis or following significant incidents or significant changes to operations or risks.

GUIDANCE

- Schedule and perform regular tests, such as quarterly fire drills and annual assessments of physical security measures.
  - Conduct both announced and unannounced tests

EXAMPLES OF EVIDENCE

- Detailed reports of the tests conducted, including objectives, procedures, results and any issues identified.
- Minutes from review meetings detailing discussions, findings and decisions regarding protection measures.

TIPS

GUIDANCE

- Consider creating a topic-specific policy for protection against physical and environmental threats.
- Deploy periodic simulations and awareness raising activities to assess the readiness of personnel and the adequacy of the procedures
- Consider implementing physically secure storage facilities for high-criticality assets of.

EXAMPLES OF EVIDENCE

- Documented physical and environmental security policy, including a description of facilities and network and information systems in scope.
- Results of periodic simulations and awareness raising activities.

13.3 PERIMETER AND PHYSICAL ACCESS CONTROL

13.3.1. For the purpose of Article 21(2)(i) of Directive (EU) 2022/2555, the relevant entities shall prevent and monitor unauthorised physical access, damage and interference to their network and information systems.

GUIDANCE

- Implement perimeter physical access control, where relevant ([109]), taking into account the measures for protection against physical and environmental threats (section 13.2).
- Ensure that physical access control is integrated with logical and network access control, in line with human resources security procedures (section 10.1) to support the detection of irregular activities and enhance overall organisational security.

EXAMPLES OF EVIDENCE

- Documented policy for physical security measures, including a description of facilities and network and information systems in scope.

13.3.2. For that purpose, the relevant entities shall:

(a) on the basis of the risk assessment carried out pursuant to point 2.1, lay down and use security perimeters to protect areas where network and information systems and other associated assets are located;

(b) protect the areas referred to in point (a) by appropriate entry controls and access points;

(c) design and implement physical security for offices, rooms and facilities,

(d) continuously monitor their premises for unauthorised physical access.

GUIDANCE

- In the risk assessment, consider risks associated with unauthorised physical access to, damage to and interference with network and information systems.

([109]) In a fully remote operating model where the organization does not maintain centralized office spaces or on-premises infrastructure, traditional perimeter and physical access control measures (e.g. badge systems, mantraps, on-site security personnel) may not be applicable. Instead, the focus should shift to ensuring that access to corporate resources is governed through strong logical access controls, such as multi-factor authentication (MFA), endpoint compliance checks and secure connectivity (e.g. VPN or Zero Trust Network Access). For personnel working from home organizations should provide guidance on securing home workspaces—such as restricting unauthorized physical access to work devices and using locked rooms or cabinets when necessary. Where third-party cloud or co-location facilities are used, physical access controls should be reviewed and enforced contractually through SLAs and verified via audit reports (e.g. ISO 27001, SOC 2).

- Based on the results of the risk assessment, determine high-criticality assets and the impact of their being compromised. This will help in identifying the perimeter for such assets.
- Prevent unauthorised physical access to facilities and set up adequate measures.
  - Physical access control measures designed to protect the entity as a whole will also protect individual assets.
  - Consider introducing further specific access control measures for specific assets or facilities.
- Consider physical security measures (indicative, non-exhaustive list):
  - physical access controls such as key cards, biometric scanners, locks and security personnel to restrict access to high-criticality areas,
  - electronic control of entry, with an audit trail,
  - segmentation of spaces or creation of zones according to authorization levels and their contents,
  - CCTV cameras and monitoring systems to continuously observe sensitive areas,
  - fencing, barriers and security patrols for securing physical perimeters,
  - guards and/or alarms to monitor every physical access point to the facility where the information system resides, 24 hours per day, seven days per week.
- Develop and enforce procedures for granting, reviewing and revoking physical access rights (section 11.2).
  - Identify a designated official within the entity to review and approve the list of personnel with authorized physical access.
  - Maintain a list of personnel with authorized access to facilities, and their authorization levels.

EXAMPLES OF EVIDENCE

- Risk assessment results
- Existence of physical security measures
- Procedures for granting, reviewing and revoking physical access rights in accordance with point 11.2 in the Annex to the regulation.

13.3.3. The relevant entities shall test, review and, where appropriate, update the physical access control measures on a regular basis or following significant incidents or significant changes to operations or risks.

GUIDANCE

- Review physical access lists.
- Employ intrusion tests that include, where applicable, unannounced attempts to bypass or circumvent measures associated with physical access points to the facility.
- At the physical boundary of the facility or network and information system, perform security checks for unauthorised exfiltration of information or removal of information system components.

EXAMPLES OF EVIDENCE

- Periodic simulations and awareness-raising activities to assess the readiness of personnel and the adequacy of the procedures for physical access control.
- Schedule and results of tests and security checks.
- Up-to-date list of personnel with authorised physical access to facilities.

TIPS

GUIDANCE

- Enforce authorisation for physical access to network and information systems in addition to the physical access controls for the facility.
- Remove individuals from the facility access list when their access is no longer required.
- Document procedures for emergencies.
- Log and monitor personnel physical access (entry and exit) through an entry control system.
- Authenticate visitors before authorizing access to the facility. Escort visitors in accordance with security policies and procedures. Maintain records of visitors' access to the facility.
- Employ automated mechanisms to facilitate the maintenance and review of visitor access records.
- Make sure that employees are aware of the existence of a secure area on a need-to-know basis.
- Define and communicate to personnel an intruder response process or emergency procedures.
- Communicate physical access control measures to employees.
- Separate facilities managed by the entity from those managed by third parties.
- Employ automated mechanisms to recognize types of intrusions and initiate defined response actions.
- Employ video surveillance of operational areas and retain video recordings for a defined period, in accordance with the GDPR.
- Keep physical access records as dictated by applicable regulations or based on an entity-defined period in accordance with the entity's policy. Keep and store physical access records in case of an audit or investigation.
- Take heed of risk-assessment results before doing anything with damaged devices containing sensitive data.

EXAMPLES OF EVIDENCE

- Perimeter incident response procedures in place.
- Personnel clearly displaying their ID.

ANNEX I

NATIONAL FRAMEWORKS

ANNEX I NATIONAL FRAMEWORKS

Belgium

Belgium has completed the incorporation of the NIS2 Directive into national legislation. In that legislation, a special role is reserved for the CyberFundamentals framework (CyFun®, www.cyfun.eu).

Finland

Traficom (the Finnish Transport and Communications Agency) has issued a national recommendation on cybersecurity risk-management measures for supervisory authorities. The Cybermeter/Kybermittari is a maturity model developed by the National Cyber Security Centre (NCSC-FI) and based on the Cybersecurity Capability Maturity Model and the NIST cybersecurity framework. They are the two instrumental documents for the national regulatory framework. The recommended cybersecurity risk-management measures are mapped to the Cybermeter/Kybermittari's objectives and practices that enable organisations to self-assess their cybersecurity capabilities and optimise their security investments. Voluntarily sharing quantitative self-assessment data to NCSC-FI enables the creation of benchmarking data and improves situational awareness of NCSC-FI.

Germany

In Germany, there is an advisory on what requirements should be seen as state of the art. The document is available at https://www.bsi.bund.de/dok/408936.

For information on BSI standards and certification, see https://www.bsi.bund.de/dok/it-grundschutz-en.

Greece

Greece has incorporated the NIS2 Directive into national legislation with Law 5160/2024. Furthermore, regarding cybersecurity measures, the Greek national framework consists of the following:

- ministerial decision 1689/2025 'National framework of cybersecurity requirements for essential and important entities';
- the *Cybersecurity Handbook*, available at https://cyber.gov.gr/wp-content/uploads/2025/04/Cybersecurity-Handbook-English-version-1.pdf;
- the self-assessment tool, available at https://cyber.gov.gr/wp-content/uploads/2025/03/Cybersecurity-Self-Assessment-Tool-English-version-1.zip.

The *Cybersecurity Handbook* and the self-assessment tool are based on globally accepted international standards and guidelines (Center for Internet Security Controls, ISO 27002, NIST 800-53, Open Worldwide Application Security Project, etc.) and will be dynamically modified to follow changes in standards, the current threat landscape and the legal and regulatory framework.

Spain

Royal Decree 311/2022, of 3 May 2022, regulates the national security framework, which is a legal regulation that is mandatory for all entities in the Spanish public sector to comply with and is mandatory to apply to the information systems used by private companies to provide services to the abovementioned public entities.

The full text of the framework is available at https://ens.ccn.cni.es/es/docman/documentos-publicos/39-boe-a-2022-7191-national-security-framework-ens/file.

ANNEX II
GLOSSARY

ANNEX II GLOSSARY

Asset: anything that is of value to the entity, including information. Overall, the assets of a network and information system are personnel, processes, information, software and hardware.

Crisis: an abnormal or extraordinary event or situation that threatens an organisation or community and requires a strategic, adaptive and timely response to preserve its viability and integrity ([110]).

Critical: one of the classification levels assigned to the entity's assets following an assessment of their criticality, including the asset classification (Annex to the regulation, point 12.1).

Cyber hygiene practices ([111])**:**

- Cyber hygiene practices for essential and important entities are a common baseline set of network and information security practices, which are already covered by the technical and methodological requirements of the cybersecurity risk-management measures outlined in the Annex to the regulation. Therefore, no additional guidance on cyber hygiene practices for essential and important entities is deemed necessary.
- Cyber hygiene practices relating to users are a set of routine, proactive practices and behaviours that the entity's users follow to maintain the network and information security of the entity's systems. These practices are explicitly mentioned in the guidance of section 8.1.

Direct suppliers and service providers: any entity providing ICT products, ICT systems or ICT services that an essential or important entity relies on. When this guidance refers to direct suppliers and service providers, it includes their personnel.

Entity: one of the relevant entities in the scope of Commission Implementing Regulation (EU) 2024/2690. In other standards or good practice guides, the term 'organisation', 'enterprise' or 'business' may be used.

Event: in reference to an information security event, an identified occurrence indicating a possible information security breach or failure of controls ([112]).

Facilities: the physical location housing the entity's network and information systems.

Incident handling: any actions and procedures aiming to prevent, detect, analyse and contain, or to respond to and recover from, an incident (NIS2 Directive Article 6(8)).

Incident: an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible through, network and information systems (NIS2 Directive Article 6(6)).

Information: data in context. In the text, we primarily use 'information', unless we refer specifically to data ('data breach' etc.).

Management bodies: the highest-level leadership within essential and important entities as in the context of Article 20 of the NIS2 Directive.

Measure: a cybersecurity risk-management measure as referred to in the NIS2 Directive. The word is used similarly to 'control', which denotes a measure that modifies risk ([113]). In addition, the terms 'measure' and 'protection measure' are used interchangeably.

([110]) ISO 22361: 2022, 3.2.
([111]) Recital 20 of the regulation addresses cyber hygiene practices for two target groups under Directive 2022/2555: essential and important entities; and their users.
([112]) ISO/IEC 27002:2022, 3.1.14.
([113]) ISO/IEC 27002:2022, 3.1.8.

Personnel: persons doing work under the entity's direction ([114]). The concept of personnel includes the entity's members, such as the governing body, management bodies, employees, temporary staff, contractors and volunteers. In this document it is used interchangeably with the term 'employees'.

Policy: intentions and direction of an organisation, as formally expressed by its management bodies.

Privileged access: the necessary permissions granted to specific users of the network and the information system of the entity, in order for them to perform tasks that regular users cannot.

Procedure: a specified way to carry out an activity or a process ([115]). The entity can document its needs for more detailed information in a way that is efficient for it beyond the policy. These are mainly procedures and processes.

Process: an activity that transforms input into output.

Rule: accepted principle or instruction that states the entity's expectations of what is required to be done and what is allowed or not allowed. Rules can be formally expressed in topic-specific policies and in other types of documents ([116]).

Significant incident: an incident that meets the criteria of Article 3 of the regulation.

Suspicious event: an event that appears unusual or a previously unknown situation that might be a potential security threat. To make clearer the difference between an event and a suspicious event, consider an example where a legitimate user fails to log in once due to a typing error. This is an event. However, a situation where a user fails to log in after five attempts might be considered a suspicious event.

Topic-specific policy: a policy on a specific subject or topic, as formally expressed by the management bodies relevant to the topic.

User: all legal and natural persons that have access to the entity's network and information systems (recital 10 of the regulation).

([114]) ISO/IEC 27002:2022, 3.1.20.
([115]) ISO 30000:2009, 3.12.
([116]) ISO/IEC 27002:2022, 3.1.32.

TP-01-25-012-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-704-7
doi: 10.2824/2702548