EUROPEAN UNION AGENCY
FOR CYBERSECURITY

IMPLEMENTING GUIDANCE

On **Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024** laying down rules for the application of Directive (EU) 2022/2555 as regards **technical and methodological requirements of cybersecurity risk-management measures**

with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

DRAFT FOR PUBLIC CONSULTATION

OCTOBER 2024

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.

CONTACT

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

AUTHORS

Konstantinos Moulinos, Marianthi Theocharidou, ENISA

ACKNOWLEDGEMENTS

This implementation guidance was developed by ENISA, in collaboration with the European Commission and the NIS Cooperation Group. ENISA would like to thank for their efforts the NIS Cooperation Group work streams on cybersecurity risk and vulnerability management, on digital service providers and on digital infrastructures, as well as the ENISA European Competent Authorities for Trust Services (ECATS) Expert Group and the European Competent Authorities for Secure Electronic Communications (ECASEC).

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.
ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.
Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.
Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.
ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN SHOULD BE PLACED HERE, DOI SHOULD BE PLACED HERE (IF APPLICABLE)

EXECUTIVE SUMMARY 5

INTRODUCTION 6

BACKGROUND 6

STRUCTURE 6

TOPIC SPECIFIC POLICIES 8

1. POLICY ON THE SECURITY OF NETWORK AND INFORMATION 9

1.1 POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS 9

1.2 ROLES, RESPONSIBILITIES AND AUTHORITIES 12

2. RISK MANAGEMENT POLICY 16

2.1 RISK MANAGEMENT FRAMEWORK 16

2.2 COMPLIANCE MONITORING 21

2.3 INDEPENDENT REVIEW OF INFORMATION AND NETWORK SECURITY 23

3. INCIDENT HANDLING 26

3.1 INCIDENT HANDLING POLICY 26

3.2 MONITORING AND LOGGING 29

3.3 EVENT REPORTING 34

3.4 EVENT ASSESSMENT AND CLASSIFICATION 36

3.5 INCIDENT RESPONSE 38

3.6 POST-INCIDENT REVIEWS 41

4. BUSINESS CONTINUITY AND CRISIS MANAGEMENT 44

4.1 BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN 44

4.2 BACKUP MANAGEMENT 48

4.3 CRISIS MANAGEMENT 52

5. SUPPLY CHAIN SECURITY 57

5.1 SUPPLY CHAIN SECURITY POLICY 57

5.2 DIRECTORY OF SUPPLIERS AND SERVICE PROVIDERS 63

6. SECURITY IN NETWORK AND INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE 65

6.1 SECURITY IN ACQUISITION OF ICT SERVICES, ICT SYSTEMS OR ICT PRODUCTS 65

6.2 SECURE DEVELOPMENT LIFE CYCLE 68

6.3 CONFIGURATION MANAGEMENT 71

6.4 CHANGE MANAGEMENT, REPAIRS AND MAINTENANCE 74

6.5 SECURITY TESTING 78

6.6 SECURITY PATCH MANAGEMENT 81

6.7 NETWORK SECURITY 83

6.8 NETWORK SEGMENTATION 87

6.9 PROTECTION AGAINST MALICIOUS AND UNAUTHORISED SOFTWARE 90

6.10 VULNERABILITY HANDLING AND DISCLOSURE 92

7. POLICIES AND PROCEDURES TO ASSESS THE EFFECTIVENESS OF CYBERSECURITY RISK-MANAGEMENT MEASURES 96

8. BASIC CYBER HYGIENE PRACTICES AND SECURITY TRAINING 99

8.1 AWARENESS RAISING AND BASIC CYBER HYGIENE PRACTICES 99

8.2 SECURITY TRAINING 101

9. CRYPTOGRAPHY 104

10. HUMAN RESOURCES SECURITY 108

10.1 HUMAN RESOURCES SECURITY 108

10.2 VERIFICATION OF BACKGROUND 110

10.3 TERMINATION OR CHANGE OF EMPLOYMENT PROCEDURES 112

10.4 DISCIPLINARY PROCESS 114

11. ACCESS CONTROL 116

11.1 ACCESS CONTROL POLICY 116

11.2 MANAGEMENT OF ACCESS RIGHTS 119

11.3 PRIVILEGED ACCOUNTS AND SYSTEM ADMINISTRATION ACCOUNTS 121

97 11.4 ADMINISTRATION SYSTEMS 124

98 11.5 IDENTIFICATION 125

99 11.6 AUTHENTICATION 127

100 11.7 MULTI-FACTOR AUTHENTICATION 131

101 12. ASSET MANAGEMENT 133

102 12.1 ASSET CLASSIFICATION 133

103 12.2 HANDLING OF ASSETS 135

104 12.3 REMOVABLE MEDIA POLICY 136

105 12.4 ASSET INVENTORY 138

106 12.5 DEPOSIT, RETURN OR DELETION OF ASSETS UPON TERMINATION OF EMPLOYMENT 141

107 13. ENVIRONMENTAL AND PHYSICAL SECURITY 143

108 13.1 SUPPORTING UTILITIES 143

109 13.2 PROTECTION AGAINST PHYSICAL AND ENVIRONMENTAL THREATS 145

110 13.3 PERIMETER AND PHYSICAL ACCESS CONTROL 148

111 ANNEX I NATIONAL FRAMEWORKS 151

112 ANNEX II GLOSSARY 152

EXECUTIVE SUMMARY

Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024[1], with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (the relevant entities) lays down the technical and the 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 of the implementing regulation.

This document offers guidance to support relevant entities to implement these technical and methodological requirements. For these requirements, the document contains:

- guidance, i.e., indicative and actionable advice on parameters to consider when implementing a requirement or further explanation to concepts found in the legal text;
- examples of evidences, i.e. the types of evidence that a requirement is in place;
- extra general tips for additional consideration by the entity, where available; and
- mapping correlating each requirement to European and international standards and national frameworks.

This guidance was prepared by ENISA, in collaboration with the European Commission and the NIS Cooperation Group. This is a living document because it maps the technical and methodological requirements, referred to in Article 2 and the Annex of the implementing regulation, to international standards as well as to national cybersecurity management frameworks which are both constantly subject to change. Therefore, a review process should be initiated at regular intervals by ENISA in collaboration with the European Commission and the NIS Cooperation Group.

DISCLAIMER

The document is not legally binding and it is only of advisory character. It does not intend to replace the frameworks, guidance or other mechanisms provided by Member States’ national law.

It should be clarified that the Member States retain the freedom to determine their approach to supervision of the requirements under this implementing regulation. Therefore, the ENISA document isn’t 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). However, the ENISA document can help the national competent authorities develop their approach to the supervision of the requirements.

Furthermore, entities in scope should check under whose jurisdiction they fall, and follow any guidance produced by national competent authorities (see Recital (7) of the Implementing regulation).

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

INTRODUCTION

BACKGROUND

On 18 October 2024, the European Commission published the 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 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), ENISA can support relevant entities by providing guidance on the implementation of the technical and methodological requirements referred to the Annex of the Regulation. This implementation guidance was developed by ENISA and the work stream on cybersecurity risk and vulnerability management of the NIS Cooperation Group (NIS CG), in collaboration with the NIS Cooperation Group work streams on digital service providers and on digital infrastructures, as well as with the ENISA European Competent Authorities for Trust Services (ECATS) Expert Group and the European Competent Authorities for Secure Electronic Communications (ECASEC). It is the result of consultations which took place from June to mid-October 2024.

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

Beyond the relevant entities to the Regulation, this guidance may provide indications on the technical and the methodological requirements of the cybersecurity risk-management measures of NIS 2 Directive, which may be considered useful by other public or private actors in improving their cybersecurity.

STRUCTURE

The Annex of the Regulation consists of 13 Titles with a varying number of technical and methodological requirements. Each technical and methodological requirement is highlighted in blue and is included in this document for readability. This is mandatory and must be implemented in its entirety by the relevant entities.

Each technical and methodological requirement is followed by three elements: guidance, examples of evidences and tips[2]. This part of the document is not legally binding and has only a recommendation character[3].

1. The **Guidance** section contains indicative and actionable advice on parameters to consider when implementing a technical and methodological requirement or further explanation to concepts found in the legal text.
2. **Examples of evidences** are indicative types of evidence that a technical and methodological requirement is in place.
3. In some technical and methodological requirements, extra general **tips** are also offered for additional consideration by the entity.

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. Entities may choose alternative methods to fulfil a requirement or use different evidence to demonstrate compliance. Moreover, a single piece of evidence may

[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.

support various requirements; for example, an organizational chart can demonstrate both 'roles and responsibilities' and 'segregation of duties.' Consequently, evidence may appear multiple times within the text.

Finally, a **mapping table** correlates each requirement with European and international standards or frameworks (ISO/IEC 27001:2022, ISO/IEC 27002:2022[4], NIST Cybersecurity Framework 2.0, ETSI EN 319 401 V2.2.1 (2018-04), CEN/TS 18026:2024), and with national frameworks[5]. It should be noted that the mapping was done only to horizontal standards and for specific topics, there are detailed standards or technical specifications referenced, where available, in footnotes. Annex I of this document provides details for each national framework submitted to ENISA during the consultation phases while in annex II some terms are explained. The document does not aim at establishing a new standard nor to duplicate existing ones (e.g., ISO, IEC, CEN). The guidance is written in a technology-neutral and standards-neutral way.

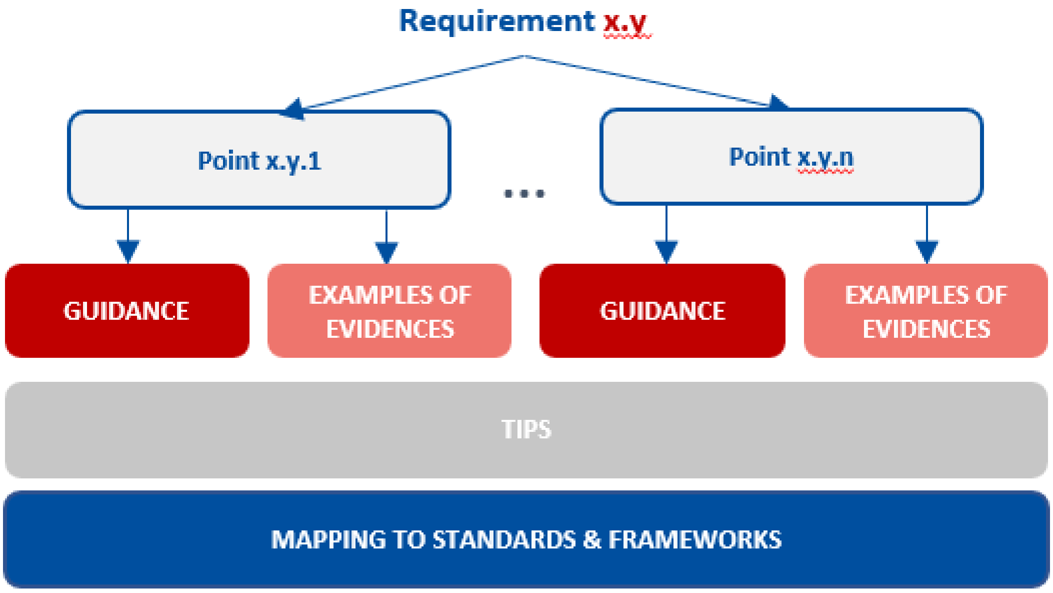

Figure 1: Technical and methodological measure structure

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.

Entities subject to the Regulation can use national frameworks, guidance, or other mechanisms equivalent to the requirements of the Regulation to demonstrate their compliance to national competent authorities. Depending on the national framework, assessment by relevant accredited conformity assessment bodies or by independent auditors authorised by the national competent authorities, against the national frameworks, guidelines or other mechanisms equivalent to technical and methodological requirements for cybersecurity risk management measures, could serve as demonstration of compliance with the requirements set out by the implementing act. In order to keep the current guidance up to date, Member States can inform ENISA of those equivalent national frameworks, guidance or other mechanisms, if available.

[4] The information security controls listed in Table A.1 of the annex A of this standard, are directly derived from and aligned with those listed in ISO/IEC 27002:2022, Clauses 5 to 8 and 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.

TOPIC SPECIFIC POLICIES

As described in preamble 9 of the Regulation, the **policy on the security of network and information systems**[6] (Annex to the Regulation, point 1.1) should be the highest-level document setting out the relevant entities' overall approach to their security of network and information systems and should be approved by the management bodies of the relevant entities.

In addition to this overarching corporate policy the following topic-specific, documented policies[7] are required:

1. **Incident handling policy** (Annex to the Regulation, point 3.1.1).
2. **Supply security chain policy** (Annex to the Regulation, point 5.1.1).
3. **Security testing policy** (Annex to the Regulation, point 6.5.1).
4. **Policy to assess the effectiveness of cybersecurity risk-management measures** (Annex to the Regulation, point 7.1.1).
5. **Policy related to cryptography** (Annex to the Regulation, point 9.1.1).
6. **Access control policy** (Annex to the Regulation, point 11.1.1).
7. **Policies for the management of privileged accounts and system administration accounts** (Annex to the Regulation, point 11.3)
8. **Handling of information and assets policy** (Annex to the Regulation, point 12.2.1).
9. **Removable media policy** (Annex to the Regulation, point 12.3.1).

[6] Article 21(2), point (a) of the NIS2 Directive.

[7] 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".

1. POLICY ON THE SECURITY OF NETWORK AND INFORMATION

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 for systems, assets, and/or procedures, which are considered in scope of the policy.
- Make sure that personnel, as well as all third parties[8] (e.g. contractors, suppliers) acknowledge the policy on the security of network and information systems, typically through a signed document or digital acknowledgement, where applicable, and what it implies for their work.

EXAMPLES OF EVIDENCES

- 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) from the Annex to the Regulation.
- The policy on the security of network and information systems as well topic specific policies are approved by top management.
- The date of the formal approval by the management bodies of the relevant entities is indicated in the policy on the security of network and information systems.
- Personnel are aware of the policy on the security of network and information systems and what it implies for their work.
- Signed acknowledgement forms from contractor personnel confirming they have read and understood the security policies.
- Interview with top management to verify their involvement with information security management.

[8] Depending on the occasion third parties might mean the suppliers, service providers, the shareholders, the authorities, the customers, visitors, external interest groups and forums.

- Evidence that top management 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 to personnel to apply network and information security in accordance with the established policies and procedures; and
    - Any initiatives that indicate that management promotes 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):
    - relevant changes in legislation, best practices;
    - feedback from interested parties;
    - results of independent reviews;
    - recommendations provided by relevant authorities;
    - violations;
    - exceptions; and
    - incidents, even those affecting other similar entities in the sector
- Update the policy on the security of network and information systems as well topic specific policies accordingly to new findings that could affect the entity's approach to managing information security including:
    - changes to the information systems;
    - changes to the environment of operation;
    - problems identified during plan implementation;
    - status of preventive and corrective actions;
    - trends related to threats and vulnerabilities;
    - exceptions
    - policy violations; and known reported security incidents.
- Obtain management approval for the revised policy and the policy exceptions.

EXAMPLES OF EVIDENCES

- Review comments or change logs for the policy on the security of network and information systems as well topic specific policies.
- Logs of policy exceptions, approved by the relevant roles. Examples of such exceptions, amongst others, include the situations mentioned in article 2(2) second paragraph as well as those under recital 5 of the Regulation. Other examples (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 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.
- Documentation of 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 as well topic specific policies.
- Evidence that any updates to the policy on the security of network and information systems as well topic specific policies, as well as any policy exceptions are approved by management, and record is kept.

TIPS

GUIDANCE

- Analyse the policy on the security of network and information systems for compliance with:
  - legislative, regulatory, and contractual requirements;
  - training and awareness requirements; and
  - business continuity requirements.
- Define procedures to facilitate the implementation of the policy on the security of network and information systems and associated measures.
- Maintain a record of the management review.
- Examine documentation of post-incident reviews for significant incidents that include participation and input from top management.
- Ensure that the policy is:
  - protected in terms of confidentiality, integrity and availability;
  - managed properly so the information is complete, correct, understandable, easily identifiable and retrievable.

EXAMPLES OF EVIDENCES

- 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.
- Training material on the policy on the security of network and information systems.
- 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 top management regarding cybersecurity matters or during significant incidents.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	5.2, A.5.1, A.5.36, A.5.4, 9.3	**BE-CyFun®2023**	BASIC: ID.GV-1.1
			IMPORTANT: ID.GV-1.2, PR.IP-5.1, PR.IP-6.1, PR.PT-2.1, PR.AT-4.1
			ESSENTIAL: PR.PT-3.3, PR.PT-4.3
NIST CSF v2.0	PR.AT-02, GV.PO-01, GV.PO-02, GV.OC-03, GV.RM-03, GV.OC-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	WORKFORCE-3, PROGRAM-1, PROGRAM-2, Management activities, CRITICAL-2, ARCHITECTURE-1,
ETSI EN 319 401	REQ 6.1-02, REQ 6.1-06, REQ 6.1-07, REQ 6.1-08, REQ 6.3	**EL – Ministerial decision 1027/2019 Article 2 - paragraph 2, Article 3**	Cybersecurity handbook: Part A: 2, Part B: 1.1, 1.5, 2.1, 3.1, 4.1, 5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1, 12.1, 13.1, 14.1, 15.1, 16.1, 17.1, 18.1
			Self assessment tool: 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, 1.13, 2.1, 2.2, 3.1, 4.1, 5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1, 12.1, 13.1, 14.1, 15.1, 16.1, 17.1, 18.1, 19.1
CEN/TS 18026:2024	ISP-01, ISP-02, OPS-01, OPS-02, OPS-03	**ES- Royal Decree 311/2022**	Article 5, Article 6, Article 10, Article 12, Annex II: 3.1 Security policy

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 way that they clearly outline rights and responsibilities.
- Assign security roles and responsibilities to personnel and include these roles in the organisational chart.
- Describe and assign corresponding responsibilities regarding the following roles (or comparable equivalents): Chief Information Officer (CIO), Chief Information Security Officer (CISO) and IT security incident handling officer.
- Use guidance of major frameworks and international standards suitable for the size and business needs of the entity, including the European Cybersecurity Skills Framework (ECSF)[9].
- Formally appoint security personnel in security roles.

EXAMPLES OF EVIDENCES

- Job descriptions.
- List of security roles (CISO, DPO, business continuity manager, etc.), who occupies them and contact information.
- Formal appointment of the key security roles and responsibilities.
- List of appointments (CISO, DPO, etc.), and description of responsibilities and tasks for security roles (CISO, DPO, etc.)

[9] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

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 general personnel aware of the security roles in the entity and when each role should be contacted.
- Make third parties aware that they should comply with the entity's network and information security policy. Consider third parties, which refer to 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. Examples include suppliers, contractors, service providers, and other external partners.

EXAMPLES OF EVIDENCES

- Awareness/dissemination material for personnel explaining security roles and when/how they should be contacted.
- Service level agreements (SLAs) with third parties. These documents should explicitly state that third parties must adhere to the entity's network and information security policy, topic-specific policies and procedures.
- Formal acknowledgement letters or emails from third-parties confirming that they have received and understand the entity's network and information security policy, topic-specific policies and procedures.

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 dedicated person (e.g., Chief Information Security Officer or Information Security Manager) responsible for overseeing security matters.
- Make sure that this person has the authority and expertise to communicate effectively with management.

EXAMPLES OF EVIDENCES

- Up-to-date documentation of the structure of security role assignments and responsibilities.
- Interview with the individual to assess communication skills and authority.
- Feedback from management and other stakeholders about the individual's effectiveness in communication.
- Minutes from meetings with the management.

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

- In bigger entities, it's often practical to have dedicated information security roles (like a Chief Information Security Officer or security analysts) who focus solely on protecting the entity's data and systems.
- In smaller entities with limited resources, information security responsibilities might be distributed among existing roles. For instance, IT staff might take on security duties alongside their regular tasks.

EXAMPLES OF EVIDENCES

- 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

- Segregate conflicting duties and areas of responsibility in order to reduce opportunities for unauthorized or unintentional modification or misuse of the entity’s asset. Examples of such segregations are (indicative, non-exhaustive list):
  - (Chief) Information Security Officer from IT administrator;
  - (Cyber security) System architect from system (security) tester;
  - Identity manager from system administrator;
  - Reviewer (auditor) from the personnel or the line of authority of the area under review (see point 2.3.2 of the Annex to the Regulation); and
  - Incident responder from legal compliance team.

EXAMPLES OF EVIDENCES

- 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 changes and/or past incidents.

EXAMPLES OF EVIDENCES

- Documentation of review process, taking into account changes and past incidents.

TIPS

GUIDANCE

- Make sure the security roles are reachable in case of incidents.
- Examine the crisis management process (see section 4.3.1) or incident response procedures (see section 3.5.1) to see if they outline specific roles for top management, as appropriate.
- Make sure that each role has its deputy or that measures ensuring the continuity in case of role representative´s absence are in place.
- 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 EVIDENCES

- Documented incident response procedures (see section 3.5) include 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.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	5.3, A.5.2, A.5.3, A.5.4	**BE-CyFun®2023**	BASIC: RS.RP-1.1
			IMPORTANT: ID.AM-6.1, PR.AT-2.1, PR.AT-4.1, PR.AT-5.1, RS.CO-1.1
NIST CSF v2.0	GV.RR-02, GV.SC-02, PR.AT-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI- Kybermittari**	PROGRAM-1, PROGRAM-2, CRITICAL-2, WORKFORCE-2 WORKFORCE-3
ETSI EN 319 401	REQ 7.2.6, REQ 7.2.7, REQ 7.2.10, REQ 7.2.11, REQ 7.2.12, REQ 7.2.13, REQ 7.2.14	**EL – Ministerial decision 1027/2019 Article 2 - paragraph 2, Article 3**	Cybersecurity handbook: Part A: 2, Part B: 1.1, 2.1, 3.1, 4.1, 5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1, 12.1, 13.1, 14.1, 15.1, 16.1, 17.1, 18.1
			Self assessment tool: 1.1, 1.2, 1.3, 1.4, 1.5
CEN/TS 18026:2024	ISP-02, OIS-02	**ES-Royal Decree 311/2022**	Article 11, Article 13

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[10] 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[11]. A risk management framework is the structured approach used by an entity to identify, assess, manage, and mitigate its cyber security risks and it might be documented or not.
- Create a risk treatment plan which associates the identified risks with assets and the measures mitigating the associated risks. The plan should at least include:
  - the risk identified;
  - the assets associated with the risk;
  - the objective associated with the risk;
  - the measures associated with the objective which are mitigating the risk;
  - procedure for assessing the effectiveness of implementation of the measure(s);
  - detailed implementation timelines;
  - responsible roles; and
  - implementation costs for the measures.
- Communicate residual risks which might affect the offered services to the customers.
- Consider residual risks from third parties e.g. data breaches, unaddressed vulnerabilities, regulatory non-compliance from the third party side, over reliance on a single third party etc.
- Ensure residual risks are accepted by management 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 or, where applicable, persons who are accountable and have the authority to manage risks, approves the risk assessment results and risk treatment plan.

EXAMPLES OF EVIDENCES

- Documented risk management framework, if available.
- Documented results from previous risk assessments.
- Documented risk treatment plan which takes into account, at least, the elements (g) to (h) referred to in point 2.1.2 of the Annex to the Regulation.

[10] The remaining risk after management has implemented a risk response (ISACA).

[11] For example, the 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, last access 29 September 2024.

- Record of management or, where applicable, by persons who are accountable and have the authority to manage risks, approval of risk assessment results.
- Record of management or, where applicable, by persons who are accountable and have the authority to manage risks, approval of residual 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[11].
- 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 that their criticality is high (e.g., up to 2 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 100,000 Euros in recovery costs).
  - 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 as long as it's monitored and patched regularly).
  - time frame for responding to and recovering from incidents (e.g., a maximum of 48 hours for containment).
  - acceptance of minor incidents as part of normal operations while prioritizing major threats.

- Define risk criteria, i.e. how the entity evaluates the significance of the risks that it identifies and makes decisions concerning risks. These may include risk acceptance criteria or criteria for performing cyber security risk assessments[12].
  - Risk acceptance criteria may include (indicative, non-exhaustive list):
    - accepting risks categorized as low severity, such as minor data leaks that don't expose sensitive information risk 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 50,000 Euros accepted without further action).
    - accepting risks after informing stakeholders and receiving their agreement, particularly if they understand the trade-offs involved.
    - 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).
  - Criteria for performing cyber security risk assessments refer to consequences, likelihood or level of risk. These may refer to (indicative, non-exhaustive list):
    - Importance of assets
    - Severity of threats
    - Vulnerability of network and information systems
    - Impact analysis
    - Frequency of cyber incidents
    - Existing measures
    - Stakeholders concerns or requirements
- Make a list of the main risks for the security of network and information systems, taking into account main threats to the assets in scope.
- Make sure that each risk is associated with at least one:
  - of the risk treatment option or a combination of them, in line with the results of the risk assessment and be 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.

[12] More information on risk criteria can be found on ISO/IEC 27005:2022, par. 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.

- Develop risk treatment plans to address the elements points (i) and (j) referred to 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 EVIDENCES

- Documented cybersecurity risk management process which takes into account elements referred to in point 2.1.2 of the Annex to the Regulation.
- Documented risk management methodology and/or tools which takes into account, at least, the elements (a) to (f) referred to in point 2.1.2 of the Annex to the Regulation.
- List of main risks described at a high level, including the underlying threat(s), 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, natural or man-made, accidental or intentional).
- Evidence that residual risks resulting from dependencies on third parties are listed and mitigated.

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 the personnel takes into account the elements referred to in point 2.1.3 of the Annex to the Regulation.

EXAMPLES OF EVIDENCES

- Guidance for personnel on assessing risks which 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;
  - changes to the information systems;
  - changes to the environment of operation;
  - post-incident review findings (3.6); and
  - trends related to threats and vulnerabilities.

EXAMPLES OF EVIDENCES

- Documentation of review process, taking into account the points mentioned in the middle column.
- Review comments or change logs for risk assessment and risk treatment plan.

TIPS

GUIDANCE

- Ensure that key personnel uses the risk management methodology and tools.
- Mitigate residual risks, where possible.
- Overall the entity has four risk treatment options associated with each risk. Each option should be accompanied by specific risk treatment measure (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: As a measure to treat this risk the entity might choose to shift the risk to another party, typically through insurance or outsourcing certain functions to a third-party provider. For instance, purchasing cyber insurance to cover potential data breach costs.
  - 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 materializes.
- Make sure that the risk from vulnerabilities assigned to the highest classification (e.g. ”critical” in CVSS) or equivalent is not accepted, if possible (6.10)
- Concerning the risk treatment plans, the entity might additionally take account:
  - findings of the review;
  - implementation steps; and
  - resources needed.
- Manage any exceptions in the risk treatment plans’ implementation.

EXAMPLES OF EVIDENCES

- Documented action plans developed in response to review findings.
- Key personnel knows the main risks .
- Documented risk treatment plan implementation exceptions

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	6.1, 6.1.2, 6.1.3, 6.2, 8.2, 8.3, A5.7, A.5.19, A.5.20, A.5.21	**BE-CyFun®2023**	BASIC: ID.GV-4.1, ID.RA-5.1
			IMPORTANT: ID.BE-4.1, ID.GV-4.2, ID.RA-5.2, ID.RA-6.1, ID.RM-1.1, ID.RM-2.1, ID.RM-3.1, ID.SC-2.1, ID.SC-3.1, PR.AC-7.1, DE.CM-6.2, RS.MI-1.1
			ESSENTIAL: ID.RA-5.3, ID.SC-1.1, PR.AC-1.5, DE.AE-4.1
NIST CSF v2.0	ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-03, ID.RM-01, GV.RM-06, GV.RR-03, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	CRITICAL-2, RISK-1, RISK-2, RISK-3, RISK-4, RISK-5, THIRD-PARTIES-2, WORKFORCE-3, WORKFORCE-4
ETSI EN 319 401	REQ 5, Clause 6.3	**EL – Ministerial decision 1027/2019 Article 4 - paragraphs 3, 4**	Cybersecurity Handbook: Part A: 2
			Self assessment tool: 1.15, 1.16, 1.17, 1.18, 1.19
CEN/TS 18026:2024	OIS-01, RM-01, RM-02, RM-03	**ES-Royal Decree 311/2022**	Article 7, Article 14

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 the management bodies. Consider the following elements (indicative, non-exhaustive list):
  - key metrics;
  - compliance status;
  - identified risks, and
  - recommended actions.
- Reports are generated and presented to management bodies at least annually.

EXAMPLES OF EVIDENCES

- Recent compliance review reports.

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

- Review Set up procedures for compliance monitoring, including (indicative, non-exhaustive list):

  - objectives and high-level approach of compliance monitoring;
  - relevant security policies that are subject to compliance monitoring;
  - frequency of compliance reviews;
  - who should carry out compliance reviews (in- or external); and
  - templates for compliance review reports.
- Analyse and evaluate the results of the compliance review.

EXAMPLES OF EVIDENCES

- Documented procedures for monitoring compliance.
- Documented analysis and evaluation of the results, including the current state of the entity's management of risks.
- 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 yearly, taking into account:
  - significant incidents, if any;
  - changes to the environment of operation
  - changes to the threat landscape and cyber security legal and regulatory requirements; and
  - changes to the policy on the security of network and information systems and/or topic specific policies.

EXAMPLES OF EVIDENCES

- Any corrective actions resulting from the assessments and tests, including the changes to the measures made by the entity once effectiveness of measures has been assessed in line with Annex to the Regulation, point 7.1.1

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	9.2, A.5.31, A.5.35, A.5.36	**BE-CyFun®2023**	BASIC: RS.IM-1.1
			IMPORTANT: ID.GV-1.2, ID.GV-3.2, ID.SC-4.1, PR.AT-3.3, PR.IP-9.1, DE.DP-3.1, DE.DP-5.1, RS.IM-1.2, RS.IP-2.1, RC.IM-1.1
			ESSENTIAL: ID.SC-4.2, PR.AT-3.4, PR.IP-7.2, PR.IP-9.2, DE.DP-5.2
NIST CSF v2.0	GV.OV-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	PROGRAM-1, PROGRAM-2
ETSI EN 319 401	Clause 7.13	**EL – Ministerial decision 1027/2019 Article 4 - paragraphs 1, 6**	Cybersecurity Handbook: Part A: 2
			Self assessment tool: 1.11, 1.12, 1.19, 1.20

CEN/TS 18026:2024	CO-01, DOC-03, INQ-01, INQ-02, INQ-03	**ES-Royal Decree 311/2022**	Article 28, Article 31, Article 32, ANNEX III - Security audit[13]

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 an entity with the appropriate competences (indicative, non-exhaustive list):
  - cybersecurity technical knowledge e,g. cybersecurity frameworks (ISO/IEC 27001, NIST etc);
  - the industry knowledge;
  - risk assessment skills;
  - compliance and regulatory knowledge e.g. the NIS2, GDPR, DORA etc; and
  - good understanding of good practices in auditing.

EXAMPLES OF EVIDENCES

- Evidences on the competences of the independent reviewers e.g. certifications like CISA, CISSP, CISM, working experience, academic qualifications, 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);
  - review committee's role;
  - frequency of the independent reviews;
  - who should carry out independent reviews (in- or external, independence is important); and
  - templates for independent review reports.
- Maintain independence in line with point 2.3.2 of the Annex to the Regulation;
- If the size of the entity makes the separation of line of authority challenging, consider alternative measures (indicative and non-exhaustive list):
  - review personnel rotation;
  - setting up a review committee with members from different departments;
  - external third-party review service provider.

[13] As a development of the National Security Framework (ENS), two Resolutions have been published by the Secretary of State for Civil Service which regulate the ENS Compliance and the ENS Security Audit process. They an be found at: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-4573 (ENS security Audit) and https://www.boe.es/diario_boe/txt.php?id=BOE-A-2016-10109 (ENS Compliance)

EXAMPLES OF EVIDENCES

- 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.
- Develop a standardized report format for reporting to the management bodies. Consider the following elements (indicative, non-exhaustive list):
  - executive summary, including the scope and the 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.

EXAMPLES OF EVIDENCES

- Documented analysis and evaluation of the results, including any residual risks.
- Minutes from review committee's gathering from past reviews.
- Any corrective actions resulting from the assessments and tests, including the changes to the measures made by the entity once effectiveness of measures has been assessed in line with the Annex to Regulation, point 7.1.1
- Documentation of any corrective actions.
- Most recent results of compliance monitoring and auditing.

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

- Make sure that independent review is conducted in the defined frequency.
- Independent reviews should take place at least yearly, taking into account:
  - significant incidents, if any;
  - changes to the environment of operation
  - changes to the threat landscape and cyber security legal and regulatory requirements; and
  - changes to the policy on the security of network and information systems and/or topic specific policies.

EXAMPLES OF EVIDENCES

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

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	9.2, 10.1, A.5.35, A.8.34	**BE-CyFun®2023**	ESSENTIAL: ID.SC-4.2, PR.IP-7.2, DE.DP-5.2, DE.CM-2.2
NIST CSF v2.0	GV.OV-02, ID.IM-01	**FI-Kybermittari**	PROGRAM-2
ETSI EN 319 401	Clause 7.13	**EL**	Cybersecurity Handbook: -
			Self assessment tool: 15.2
CEN/TS 18026:2024	CO-01, CO-02, CO-03, CO-04	**ES-Royal Decree 311/2022**	National Security Framework Compliance, sections V (National Security Framework Compliance) and VI (Requirements of the certifier bodies)

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[14].

EXAMPLES OF EVIDENCES

- Documented incident handling policy which contains, at least, the elements referred to in point 3.1.2 of the Annex to the Regulation.
- Documented standards and/or good practices which 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 (4.1) by (indicative, non-exhaustive list):
  - ensuring that they aim to minimise disruptions, protect assets, and ensure a swift return to normal operations;
  - describing workflows which trigger business continuity (4.1 or 4.2 or 4.3) during an incident; and
  - developing scenarios that test the interaction between these processes.
- 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 to categorise events as incidents[15]. An indicative, non-exhaustive list of criteria might include one or more of the following:
  - impact on business operations;
  - data sensitivity in accordance with the GDPR;
  - legal and regulatory impact;

[14] Additionally to the frameworks in the mapping table, consider “Computer Security Incident Handling Guide” from NIST, available at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf, last accessed 12.10.2024.

[15] 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 categorization of incidents, please also consult the ENISA guidelines related to Article 23(9) summary reporting for NIS2 or information provided by the national CSIRTs.

    - scope and scale meaning the evaluation of how widespread the event is;
    - type of the attack;
    - malicious software/vulnerability exploitation;
    - criticality of the systems affected;
    - incident containment urgency;
    - potential of data exfiltration or corruption e.g. in case of ransomware;
    - likelihood of recovery; and
    - impact on human lives and safety
- Ensure that the incident handling policy refers to different types of incidents like (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 (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;
    - conditions and procedures for escalation of incidents;
    - channels to be used for communication (e.g., email, intranet, phone calls, social media, press releases);
    - methods for stakeholders to provide feedback or ask questions; and
    - guidelines for when to communicate and the frequency of updates, as well as pre-drafted message templates for various scenarios and the core messages to be communicated
- Additional to the elements referred to in point 3.1.2 of the Annex to the Regulation, describe in the incident handling policy how it interacts with the business continuity and disaster recovery plan.

EXAMPLES OF EVIDENCES

- Cross references between incident handling policy, business continuity and disaster recovery plan.
- 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.
- A communication plan for incident handling is in place.
- Procedures on how to communicate the incident to relevant authorities and the CSIRT are in place.
- Procedures on 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 in order 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;
  - log analysis exercise; and
  - past incident walkthrough.
- Test roles, responsibilities and procedures laid down in the policy at least semi-annual.
- Review and update roles, responsibilities and procedures laid down in the policy at least yearly, taking into account, additionally 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 cyber security legal and regulatory requirements; and
  - changes to the policy on the security of network and information systems and/or topic specific policies.

EXAMPLES OF EVIDENCES

- 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.

TIPS

GUIDANCE

- Identify and consider all internal and external resources required in case 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) 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 fulfill under different reporting regimes.

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5 .24	**BE-CyFun®2023**	BASIC: RS.RP-1.1
			IMPORTANT: ID.AM-6.1, PR.IP-9.1, RS.CO-1.1, RS.MI-1.1, RC.RP-1.1
NIST CSF v2.0	GV.SC-08, RS.MA-01, RS.MA-05, RS.MI-01, RS.MI-02, ID.IM-01, ID.IM-04	**FI-Kybermittari**	RESPONSE-1, RESPONSE-2, RESPONSE-3, RESPONSE-5, CRITICAL-3
ETSI EN 319 401	REQ-7.9-06	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 18**	Cybersecurity Handbook: Part B: 17.1
			Self-assessment tool: 18.1
CEN/TS 18026:2024	ISP-02, IM-01, IM-07	**ES-Royal Decree 311/2022**	Article 25, Article 33, Article 34, Annex II: 4.3.7, 4.3.9, 4.7.2

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 the monitoring the activities on entity’s network and information systems, (indicative, non-exhaustive list):
  - threat detection;
  - compliance assurance;
  - incident response support;
  - performance optimisation;
  - anomaly detection;
  - data loss prevention; and
  - network health monitoring.
- Procedures should describe (indicative, non-exhaustive list):
  - objectives;
  - data for collection;
  - analysis of data algorithms; and
  - notification, to the relevant personnel, mechanisms.
- Select tools which serve the objectives of monitoring according to specific criteria (indicative, non-exhaustive list):
  - ease of use;
  - integration with the existing network and information system;
  - minimisation of manual intervention;
  - capability of collecting data from various sources e.g. networks, systems, applications;
  - security features offered e.g. encryption, access control; and
  - costs and licencing.

EXAMPLES OF EVIDENCES

- Procedures are in place.

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

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):
  - analytics and machine learning algorithms;
  - continuous update of 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.

EXAMPLES OF EVIDENCES

- Acceptable, in line with the state of the art, log monitoring, collection, storage and analysis tools.
- SIEM systems are used to analyse data and identify deviations from established baselines.
- Mechanisms which aim at minimising false positives and false negatives are in place.

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 entity's network and information system. These configurations are vital because any changes or misconfigurations might have significant impact, including system outages, security vulnerabilities, or reduced performance of entity's network and information system.

EXAMPLES OF EVIDENCES

- Log files contain the elements referred to in point 3.2.3 of the Annex to the Regulation.

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

- Make sure that the implemented procedures are able 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 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: 3 or more account lockouts within 15 minutes;
  - Privileged access: 2 or more instances of privilege escalation (e.g., normal user to admin) within 24 hours;
  - Antivirus: three or more malicious software detections on different devices within 30 minutes.
  - Use of system resources: three or more installations of unauthorised software within 30 minutes.

EXAMPLES OF EVIDENCES

- Regular reports which summarize log data and highlight any anomalies detected.
- Alarm thresholds are set.
- Records from past alarm triggers when thresholds were exceeded.
- Existing workflows which trigger event reporting (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 according to business needs, the risk assessment results, good practices and legal requirements/obligations.
- The backup logs' maintenance period shouldn't be shorter than the review period of the logs, 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 retention period ends.
- Consider mechanisms to protect logs from unauthorised access or changes (indicative, non-exhaustive list):
  - encryption;
  - access control;

  - hashing; 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 EVIDENCES

- A retention period is set.
- 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 review period of the logs, referred to in point 3.2.4 of the Annex to the Regulation.
- Centralised log management is in place.
- Logs do not contain data of which retention periods has 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 the time synchronisation:
  - utilize Network Time Protocol (NTP) servers or Precision Time Protocol (PTP) for accurate and reliable time synchronization[16],
  - use authenticated NTP to prevent malicious entities from tampering with your time synchronization;
  - configure a central time server within the entity. This server should synchronize with an external reliable time source and then distribute the time to all other systems within the network; and
  - use multiple time sources to avoid a single point of failure.
- 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.
- Ensure redundant log storage (e.g. cloud, multiple servers, multiple storage locations) to prevent data loss in line with what is referred to in point 4.2 of the Annex to the Regulation.
- Deploy separate tools to monitor the health and availability of entity's primary monitoring and logging systems.

EXAMPLES OF EVIDENCES

- Mechanisms for logs' time synchronisation are in place.
- Mechanisms for logs' redundant storage are in place.
- Logs from the activity of the tools which monitor the health and availability of entity's primary monitoring and logging systems

[16] For public NTP servers see https://ntp.org/

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. assets.

EXAMPLES OF EVIDENCES

- Review plans or schedules.

TIPS

GUIDANCE

- 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 which are included in the logs is not processed unnecessarily. When required, 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 capabilities (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 e.g. JASON and XML;
  - log level in line with the classification level of the asset being logged. The entity should assign a higher level of log level e.g. ERROR, FATAL to highly classified assets while the lower log levels e.g. INFO, DEBUG should be used for assets with lower classification; and
  - the standard for the timestamps e.g. ISO-8601
- For each log entry should contain necessary metadata such as (indicative, no exhaustive list):
  - log level;
  - timestamp;
  - source identifier e.g. the application or the device relevant to the entry; and
  - a unique identifier for the entry.

EXAMPLES OF EVIDENCES

- Documented procedures.
- Log baselines are in place.
- Each entry contains necessary metadata.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.28, A.8.15, A.8.16, A.8.17	**BE-CyFun®2023**	BASIC: PR.PT-1.1, DE.AE-3.1
			IMPORTANT: PR.AC-2.2, PR.AC-4.5, PR.DS-5.1, PR.IP-7.1, PR.MA-1.3, DE.AE-3.2, DE.CM-1.2, DE.CM-6.1, DE.CM-7.1
			ESSENTIAL: ID.SC-3.2, PR.PT-1.3, DE.AE-1.1, DE.AE-3.3, DE.CM-1.3, DE.CM-2.2
NIST CSF v2.0	RS.AN-06, RS.AN-07, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	SITUATION-1, SITUATION-2, SITUATION-3, ASSET-4
ETSI EN 319 401	REQ-7.9-01, REQ-7.9-02, REQ-7.9-03, REQ-7.9-04, REQ-7.9-09, REQ-7.9-12	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 17**	Cybersecurity Handbook: Part B: 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10
			Self-assessment tool: 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10, 9.11
CEN/TS 18026:2024	OPS-10, OPS-11, OPS-12, OPS-13, OPS-14, OPS-15, OPS-16, OPS-23, CS-01, IM-07, PSS-01	**ES-Royal Decree 311/2022**	Article 10, Article 21, Annex II: 4.7.1, 4.7.3

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):
  - the confidentiality or the integrity or the availability (CIA) of the network or the information system has been affected;
  - persistence meaning if the event is ongoing or not;
  - impact e.g. the number of assets (potentially) affected, the financial impact for the entity etc; 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, in case that the event is notified in accordance with the NIS2 articles 23 or 30. As a 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 these channels are easily accessible and intuitive to use.

EXAMPLES OF EVIDENCES

- Documented mechanism that outlines the process for reporting security events.

- Examples or templates of reporting.[17]
- Personnel is aware of the mechanism and who to contact in case they notice something or suspicious.
- Existence of multiple reporting channels such as email addresses, web forms, phone numbers, or dedicated reporting portals.

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 available to personnel, entity's suppliers and customers, appropriate means and time thresholds for reporting.
- Consider anonymous reporting to encourage individuals to report security events without fear of reprisal.
- Take into account legal obligations for time thresholds to report an incident to competent authorities (and CSIRTs) in line with NIS2 articles 23 and 30.
- 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 EVIDENCES

- 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, 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 reporting mechanism.
- Periodic simulations and awareness raising activities to assess the readiness of personnel and the adequacy of the mechanism to report 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 (3.1.2), based on changes or past events.

EXAMPLES OF EVIDENCES

[17] Seek coherence with the reporting templates required by the national CSIRT or where applicable the competent authority.

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks			
ISO 27001:2022	A.6.8	**BE-CyFun®2023**	BASIC: PR.AT-1.1, DE.CM-3.1
			IMPORTANT: PR.AT-1.2, DE.AE-3.2, DE.AE-5.1, DE.CM-2.1, RS.CO-1.1, RS.CO-5.1
			ESSENTIAL: DE.AE-1.1, DE.AE-3.3, DE.CM-1.3, RS.CO-2.2
NIST CSF v2.0	RS.MI-01, RS.CO-02	**FI-Kybermittari**	RESPONSE-1, WORKFORCE-2
ETSI EN 319 401	REQ-7.9-06, REQ-7.9-07, REQ-7.9-08	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 18**	Cybersecurity Handbook: Part B: 17.2, 17.7
			Self-assessment tool: 18.3
CEN/TS 18026:2024	IM-03, IM-04	**ES-Royal Decree 311/2022**	Article 32, Article 33, Annex II: 4.3.7

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 (section 3.1.1 of this guideline 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 EVIDENCES

- Defined criteria are in place.
- An incident categorisation system.

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

- Document procedures for assessing suspicious events to determine their nature and severity. These procedures 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 or runbooks to guide initial assessment and response actions for common types of incidents e.g. ransomware, phishing, data or device loss, fire.
- Classify events based on their nature, severity, and potential impact. Common classifications may include:
  - low, medium, or high severity.
  - incident types (e.g., malicious software infection, 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.
- Determine recurring instances of an incident by performing root cause analysis[18].
  - Consider that the root cause of an incident may challenging to determine at 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 in order to improve processes, procedures and thresholds.

EXAMPLES OF EVIDENCES

- 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 past event assessment and classification to improve processes, procedures and thresholds.

TIPS

GUIDANCE

- Consider deploying a Security Information and Event Management tool (SIEM), or similar systems that will allow and facilitate the correlation and analysis of data.
- Utilize automation where possible to triage incoming alerts and prioritize them based on severity and potential impact.
- 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 that only collect and analyse logs that fit the purpose. Avoid retaining unnecessary personal or sensitive data;
  - anonymising or pseudonymising , when possible, the collected data;

[18] More information on root cause analysis can be found at:
FIRST Computer Security Incident Response Team (CSIRT) Services Framework, Version 2.1, 6.2.4 Function: Information security incident root cause analysis, available at https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1#6-Service-Area-Information-Security-Incident-Management

- ○ apply good security practices when applicable and relevant such as access control, encryption, regular audits and monitoring;
- ○ apply the data retention policy in alignment with the GDPR requirements and regularly purge data that is no longer needed; and
- ○ considering the data protection and other than NIS2 relevant legal and compliance obligations.

EXAMPLES OF EVIDENCES

- A SIEM or a similar system.
- Tools supporting incident triage.
- Measures to protect the security of information during log analysis and correlation.
- Communications with the national Data Protection Authority (DPA) concerning the data protection of the logs.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.25	**BE-CyFun®2023**	BASIC: RS.IM-1.1
			IMPORTANT: PR.IP-9.1, DE.AE-1.2, DE.AE-3.2, DE.AE-5.1, DE.DP-3.1, RS.AN-2.1
			ESSENTIAL: PR.PT-1.4, DE.AE-2.2, DE.AE-3.3, DE.AE-4.1, DE.CM-1.3, DE.DP-4.1, RS.AN-2.2, RS.AN-3.2
NISTCSF v2.0	DE.AE-04, RS.MA-02, RS.MA-03, RS.MA-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	RESPONSE-1, RESPONSE-2
ETSI EN 319 401	REQ-7.9-07, REQ-7.9-12	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 18**	Cybersecurity Handbook: Part B: 17.2
			Self-assessment tool: 18.2, 18.3
CEN/TS 18026:2024	IM-02	**ES-Royal Decree 311/2022**	Article 32, Article 33, Annex II: 4.3.7

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.
- Define roles and responsibilities within the incident response team, including incident coordinators, analysts, and communication liaisons.
- Take into account well known standards when developing the incident response procedures[19].

[19] Additionally to those mentioned in the mapping table at the end of this section, consider also the following:
a) ISO/IEC 27035-1:2023, Information technology — Information security incident management, Part 1: Principles and process.

[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

EXAMPLES OF EVIDENCES

- Assignments of roles within the incident response team.
- Documented standards and/or good practices which are taken into account.

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 detailed 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.
  - Conflicting objectives between:
    - 1) forensic activities to secure evidence,
    - 2) incident response activities to remove existing threats, and
    - 3) objectives of operational IT operations to minimise the impact of the incident,

  are considered and presented to the management bodies for a decision on how to proceed.

EXAMPLES OF EVIDENCES

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

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 (3.1.2) includes procedures on how to communicate the incident to relevant authorities and the national CSIRT as well as with the internal and external stakeholders.
- Include contact information for key personnel, external stakeholders, and relevant authorities.

EXAMPLES OF EVIDENCES

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

b) ISO/IEC 27035-2:2023, Information technology — Information security incident management, Part 2: Guidelines to plan and prepare for incident response.
c) NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, available at https://csrc.nist.gov/pubs/sp/800/61/r2/final.

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 at minimum contains (indicative, non-exhaustive list):
  - time of detection, containment and eradication;
  - when the systems recovered;
  - indicators of compromise (IoCs);
  - root cause;
  - actions taken during each phase namely, detection, containment and eradication;
  - impact assessment;
  - communications when responding to the incident;
  - post incident lessons learnt and recommendations; and
  - whether the incident was notified to the CSIRT or the competent authority according to NIS2 articles 23 and 30;

EXAMPLES OF EVIDENCES

- Logs from incident response

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

GUIDANCE

- Test entity's incident response procedures at least annually.
- Test different types of incidents e.g. ransomware, phishing, data breach, DoS, etc.
- Ensure that test scenarios involve employees from different departments as well as external stakeholders e.g. suppliers and service providers.
- 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 EVIDENCES

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

TIPS

GUIDANCE

- Instructions on how to respond to the most common types of incidents (e.g. 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, e.g. SOAR technologies or similar systems.

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.26	**BE-CyFun®2023**	BASIC: RS.RP-1.1
			IMPORTANT: PR.IP-9.1
			ESSENTIAL: PR.IP-9.2, RS.CO-2.2
NIST CSF v2.0	RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, ID.IM-02, ID.IM-03, ID.IM-04, RS.CO-02, RS.CO-03, RS.AN-03, RS.MI-01, RS.MI-02, RC.CO-03, RC.CO-04.	**FI-Kybermittari**	RESPONSE-2, RESPONSE-3
ETSI EN 319 401	REQ-7.9-05, REQ-7.9-09, REQ-7.9-12	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 18**	Cybersecurity Handbook: Part B: 17.2, 17.3, 17.4, 17.5, 17.6, 17.9, 17.10
			Self-assessment tool: 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8
CEN/TS 18026:2024	OIS-03, IM-01, IM-05, IM-07, INQ-02, INQ-03	**ES-Royal Decree 311/2022**	Article 32, Article 33, Annex II: 4.3.7

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

- Define a process for conducting post-incident reviews after security incidents.
- Identify root causes, 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 based on logs from incident response referred to in point 3.5.4 of the Annex to the Regulation.

EXAMPLES OF EVIDENCES

- Conduct root cause analysis[18] and identify the root cause of the incident.
- 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 the risk treatment plan (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 cyber security incident or whether measures may need to be taken to restore them (e.g. resetting passwords for administrative emergency access).

EXAMPLES OF EVIDENCES

- Post-incident review reports that detail findings, lessons learnt, and recommendations for improvement following security incidents.
- Analysis, resolving and mitigation measures taken are communicated to all relevant personnel.

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 toa post-incident review.

EXAMPLES OF EVIDENCES

- 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, relevant to the incident topic specific policies, procedures, and incident handling policy and incident response procedures in light of the lessons learnt from post-incident reviews.

EXAMPLES OF EVIDENCES

- Minutes from the composition 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.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.27	**BE-CyFun®2023**	BASIC: RS.IM-1.1
			IMPORTANT: PR.P-7.1, RS.IM-1.2, RS.IM-2.1, RS.CO-1.1, RS.CO-3.2, RC.IM-1.1
NIST CSF v2.0	ID.IM-01, ID.IM-04, RS.AN-08	**FI-Kybermittari**	RESPONSE-3, RESPONSE-5
ETSI EN 319 401	-	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 8**	Cybersecurity Handbook: Part B: 17.8
			Self-assessment tool: 18.2, 18.3
CEN/TS 18026:2024	IM-06	**ES-Royal Decree 311/2022**	Article 32, Article 33, Annex II: 4.3.7

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 well known standards when developing the business continuity and the disaster recovery plan.
- Create a list of natural and/or major disasters that could affect the services together with a list of disaster recovery capabilities e.g. backups, tests, recovery objectives etc.

EXAMPLES OF EVIDENCES

- 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 business continuity plan, including:
  - decisions taken;
  - steps followed; and
  - final recovery time.
- Determine the order of recovery based on criteria (indicative, non-exhaustive list):
  - the asset classification level;
  - the importance of the service for the entity;
  - dependencies (services or assets that which are essential for others are restored first);

  - recovery objectives (point 4.1.3 of the Annex to the Regulation);
  - 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.
- Require primary and alternate telecommunications service providers, according to what is referred to in point 13.1 of the annex of the Annex to the Regulation, in order to maintain properly disaster recovery plans (for the services provided).
- Prepare for recovery and restoration of services after a disaster identifying measures like:
  - failover sites in other regions; and
  - backups of data with high criticality to remote locations.
- Make sure that third party services will be available in case of disaster (e.g. hot site).
- Implement advanced measures for disaster recovery capabilities like:
  - full redundancy;
  - failover mechanisms; and
  - alternative site.

EXAMPLES OF EVIDENCES

- Measures are in place for dealing with disasters, such as failover sites in other regions, backups of data to remote locations, et cetera.
- Up-to-date organisational structures widely communicated.
- Map 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 business impact analysis (BIA)[20] 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 (such as ICT systems and processes, respectively) after a disaster occurs.
  - Recovery point objectives (RPOs) to determine how much data can be lost by specific ICT activities or applications as a result of an outage.
  - Service delivery objectives (SDOs) to determine the minimum level of performance that needs to be reached by business functions during the alternate processing mode.
- RTOs, RPOs and SDOs may be used to determine backup and redundancy procedures.
- Document disaster recovery plan, taking into account:

[20] Consider the following standards: ISO/TS 22317:2021 and NIST Special Publication 800-34

    - the RTOs, RPOs and SDOs; and
    - compliance with applicable regulations and legislation.

EXAMPLES OF EVIDENCES

- 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.
- Test business continuity and disaster recovery plans regularly, taking into account:
    - change logs;
    - past incidents; and
    - results of previous tests.
- Test disaster recovery plan at the 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; and
    - resiliency to maintain service to customers.
- Define a 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, on order to ensure that the plans incorporate lessons learnt from such tests.
- Review and, if necessary, update roles and responsibilities.
- Review of dependent third parties' disaster recovery plans in order to ensure that the plans meet entity's business continuity requirements.
- Communicate business continuity and disaster recovery plans' changes to related key personnel.

EXAMPLES OF EVIDENCES

- 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, final recovery time.

- Communications e.g. emails, documents, intranet announcements etc concerning the changes of the business continuity and disaster recovery plans.
- Evidences e.g worklow changes, updated plans etc that lessons learnt from past tests are incorporated into the 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;
  - 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 business continuity plan registering successful and failed recovery times.
- Coordinate business continuity planning activities with incident handling activities.
- Coordinate 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.
- Periodically conduct awareness training regarding the continuity of operations for the personnel.
- Set up procedures in regards to the appropriate communication channels with the (inter)national competent authorities containing disaster management organisations and disaster-relief teams.
- Train regularly the responsible personnel in disaster recovery operations.
- Implement contingency plans for systems based on scenarios.
- Monitor activation and execution of contingency plans, registering successful and failed RTOs, RPOs and SDOs.
- Implement contingency plans for highly criticality dependent and inter-dependent sectors and services.

EXAMPLES OF EVIDENCES

- Measures e.g. encryption, access control etc 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, final recovery time.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A5.29, A. 5.30[21]	BE-CyFun®2023	BASIC: ID.BE-5.1, PR.IP-4.1
			IMPORTANT: ID.SC-5.1, PR.IP-9.1
			ESSENTIAL: ID.SC-5.2, PR.IP-4.4, PR.IP-4.5, PR.IP-9.2, RC.RP-1.2
NIST	ID.IM-02, ID.IM-03, ID.IM-04, GV.OC-04, GV.SC-08, RC.RP-01, RC.RP-02	FI-Kybermittari	RESPONSE-4, RESPONSE-5, CRITICAL-3
ETSI EN 319 401	Clause 7.11	EL – Ministerial decision 1027/2019 - Article 4 - paragraph 19, 20	Cybersecurity Handbook: Part B: 18.1, 18.2
			Self-assessment tool: 19.1, 19.2, 19.3
CEN/TS 18026:2024	BC-01, BC-02, BC-03, BC-04	ES-Royal Decree 311/2022	Article 26, Article 27, Annex II: 4.6.1, 4.6.2, 4.6.3

4.2 BACKUP 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, e.g. cloud providers, to provide such redundancy.

EXAMPLES OF EVIDENCES

- Backups are physically separated.
- In case that the service is offered by a third party, service level agreements (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.

[21] Further information on business continuity management can be found in ISO 22313: 2020 and ISO 22301:2019. Information on business impact analysis (BIA) can be found in ISO/TS 22317:2021 and in NIST IR 8286D: Using Business Impact Analysis to Inform Risk Prioritization and Response

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.

EXAMPLES OF EVIDENCES

- Backup plans.
- Logs from backup software that show regular backups are being performed.
- Backups are physically separated and are offered an appropriate level of protection, including encryption.
- Logs or reports confirming that one copy of the backup is stored offsite, such as in a cloud storage service or a remote data center.
- 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 cloud storage service to ensure they are 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;
  - 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 and functional;
  - 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 EVIDENCES

- 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 where data is restored from backups.
- Evidence of tests for different recovery scenarios, including full system restores and individual file recoveries.
- Logs or reports from actual incidents where recovery procedures were implemented (3.2 and 3.5).
- In case that the service is offered by a third party, service level agreements (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

- Network and information systems, one or more of the following (indicative, non-exhaustive list):
  - multiple internet service providers;
  - load balancing;
  - mirrored servers;
  - virtualisation; and
  - Redundant Array of Independent Disks (RAID).
- Assets, one or more of the following (indicative, non-exhaustive list):
  - shared workspaces;
  - backup locations;
  - spare equipment; and
  - multiple suppliers for the same categories of products;
- Personnel, one or more of the following (indicative, non-exhaustive list):
  - job rotation;
  - backup assignments; and
  - emergency drills;
- Multiple communication platforms e.g social media, messaging apps, email etc;

EXAMPLES OF EVIDENCES

- Oner 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 EVIDENCES

- Evidence that 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 (point 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, like business partners or customers in tests.

EXAMPLES OF EVIDENCES

- Regular testing of backup status, processes and procedures.
- Test program for backup plans, including types of contingencies, frequency, roles and responsibilities, templates and procedures for conducting tests, 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 lessons learnt from the tests.
- Issues and lessons learnt from past tests have been 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.
- Before systems or configurations are restored, a “patient zero[22]” may need to be identified so that the restoration does not restore any vulnerabilities or infections that have sometimes been cleaned up.
- 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.

EXAMPLES OF EVIDENCES

- Measures are in place to protect backup and restoration hardware and software e.g. physical access controls, surveillance systems, encryption, integrity checks, failover mechanisms etc.
- 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 cloud storage service to ensure they are configured to receive and store backup copies.

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.13, A.8.14	**BE-CyFun®2023**	BASIC: PR.IP-4.1, RC.RP-1.1
			IMPORTANT: PR.IP-4.2, PR.DS-3.3, PR.DS-5.1, PR.DS-6.1, PR.IP-4.3
			ESSENTIAL: ID.BE-5.2, PR.DS-8.1, PR.IP-4.4, PR.IP-4.5
NIST CSF v2.0	PR.DS-11, RC.RP-01, RC.RP-02, ID.IM-03	**FI-Kybermittari**	RESPONSE-4, ASSET-1, ASSET-2, CRITICAL-2, ARCHITECTURE-1, ARCHITECTURE-5
ETSI EN 319 401	-	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 12**	Cybersecurity Handbook: Part B: 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7
			Self-assessment tool: 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8
CEN/TS 18026:2024	OPS-06, OPS-07, OPS-08, OPS-09	**ES-Royal Decree 311/2022**	Annex II: 5.7.6

4.3 CRISIS MANAGEMENT

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

GUIDANCE

- Take into account well known standards when developing the crisis management process[23].
- Due to the fact that 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[24]. This may refer to incidents that cause serious impact, beyond a certain threshold of tolerance. These criteria may include (indicate and non-exhaustive list):
  - the incident poses significant risk to critical assets or operations with high criticality, e.g. high-severity incidents (e.g., data breaches involving sensitive information)
  - the incident disrupts business operations significantly, e.g. prolonged downtime, widespread loss of services, or significant impact on customer service.
  - the breadth of the incident—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 sophistication and motivations of the threat actors involved. Incidents linked to advanced persistent threats (APTs) or organised cybercrime may require 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 EVIDENCES

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

[23] Additionally to the frameworks in the mapping table, consider:
a) ISO 22361:2022, Security and resilience — Crisis management — Guidelines.
b) ENISA Best Practices for Cyber Crisis Management, available at: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management/@@download/fullReport
c) NIST Special Publication 800-61 Revision 2.

[24] 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'.

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

- The communication element might describe (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.

EXAMPLES OF EVIDENCES

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

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.
  - 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 relevant, 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.
  - 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 to contribute to the broader cybersecurity community.

EXAMPLES OF EVIDENCES

- Evidences from previous communications e.g. emails, correspondence, meeting minutes etc with CSIRTs or, where applicable, the competent authorities.

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 depending on the scope of the test:
  - Full scale-biannually;
  - Stress tests and crisis management process components-annually.
- Test the crisis management process (indicative, non-exhaustive list) by.
  - taking into account past crisis situations;
  - comparing the results of the tests to the objectives defined, for instance the recovery objectives under point 4.1.2 (f) of the Annex to the Regulation (e.g. RTOs, RPOs and SDOs); and
  - using the results of the comparison in order 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 EVIDENCES

- Documentation showing how crisis management integrates with the entity’s incident response plans (point 3.5 of the Annex to the Regulation), particularly for ICT-related incidents.
- Documents identifying potential previous crises and assessing their likelihood and 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

- The management should have approved the crisis management process.
- 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 case of a crisis; and
    - fall back procedures which describe the actions to be taken to protect essential activities or support services (e.g. alternative temporary locations for bringing process back to normal operation, recovery or restore).
- Train personnel regularly in the crisis management. Incorporate simulated events [25] into crisis management training to facilitate effective response by personnel in crisis situations.

EXAMPLES OF EVIDENCES

- Inventory of resources required for crisis management, including backup systems, alternative communication tools, and emergency supplies.
- Approved crisis management process.
- Documented and approved by the management bodies crisis communication plan is in place and communicated to all personnel. The plan, additionally to the elements referred to in point 4.3.2 of the Annex to the Regulation and the elements of the above guidance, includes at least (indicative, non-exhaustive list):
    - communication plans outlining 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 is aware of the processes and who to contact in case of crisis.
- Records from periodic simulations and awareness raising activities to assess the readiness of personnel and the adequacy of the procedures to manage a crisis.
- Records showing that crisis management team members and relevant staff have received training on the crisis management process.

[25] In its lightest form, the exercise can mean simulating the continuity and recovery procedures through discussion (so-called tabletop exercise).

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.26, A.5.29, A.5.30	**BE-CyFun®2023**	BASIC: RS.CO-3.1
			IMPORTANT: PR.IP-8.1, DE.DP-4.1, RS.CO-3.2
			ESSENTIAL: PR.IP-4.4, PR.IP-9.2, RC.CO-2.1, RS.CO-2.2
NIST CSF v2.0	RS.CO-02, RS.CO-03. PR.IR-03, DE.CM-01, ID.AM-03, DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07, DE.AE-08	**FI-Kybermittari**	RESPONSE-3, THREAT-2, CRITICAL-1, CRITICAL-3
ETSI EN 319 401	Clause 7.11, ref. to clause 17 of ISO/IEC 27002:2013	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 18, 19, 20**	Cybersecurity Handbook: Part B: 17.2, 17.10, 18.1, 18.2, 18.8
			Self-assessment tool: 18.2, 18.3, 19.2, 19.3, 19.8
CEN/TS 18026:2024	BC-03, OIS-03	**ES-Royal Decree 311/2022**	Article 26, Article 27, Annex II: 4.6.1, 4.6.2, 4.6.3, 5.7.6

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 in order 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 well known standards or good practices when developing the supply chain policy[26].
- The role of the entity might be one or more from the following[27]:
  - ICT supplier;
  - manufacturer;
  - software supplier;
  - hardware supplier;
  - Managed Service Provider (MSP);
  - Managed Security Service Provider (MSSP); and
  - user.

EXAMPLES OF EVIDENCES

- Supply chain policy.
- Supply chain policy is in line with documented standards and/or good practices.
- Evidence e.g. email, contract, announcements etc from the communication of the role of the entity to the direct suppliers and service providers.

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;
(b) he 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.

EXAMPLES OF EVIDENCES

- The policy contains the elements referred to in point 5.1.2 of the Annex to the Regulation.

[26] Additionally to those mentioned in the mapping table at the end of this section, consider also the following:
a) ISO/IEC 27036-1:2021, Cybersecurity — Supplier relationships Part 1: Overview and concepts.
b) ISO/IEC 27036-2:2022, Cybersecurity — Supplier relationships Part 2: Requirements.
c) 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/final.
d) ENISA Good Practices for Supply Chain Cybersecurity, https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity.

[27] The list aligns with the draft EU ICT Supply chain Toolbox from the NIS Cooperation Group work stream on supply chain, as of October 2024.

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

- Follow the activities of the Network and Information Systems (NIS) Cooperation Group, established by NIS2 article 14, on supply chain.[28]

EXAMPLES OF EVIDENCES

- Evidence that, relevant to the entity's business objectives, scenarios as well as recommendations of the NIS Cooperation Group are integrated into the supply chain policy.

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

- For small entities with limited bargaining power when dealing with large suppliers and service providers consider one or more of the following measures (indicative, non-exhaustive list):
  - collective bargaining or purchasing of products or services;
  - representation from an association that the entity is a member of;
  - legal advice for review and negotiating a contract; and
  - negotiating specific clauses such as the exit, pricing and service level agreements.
- Make sure that suppliers and service providers report vulnerabilities of their systems or products or services that present a risk to the security of the network and information systems of the entity.

EXAMPLES OF EVIDENCES

[28] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

- Contracts which contain the elements referred to in point 5.1.4 of the Annex to the Regulation.
- Comparison between selected contracts and the associated tenders in order 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.
- Evidences from supplier and service providers vulnerability related communications or reports

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 risk analysis before entering any agreement with suppliers and service providers taking into account the elements referred to in point 5.1.2 and 5.1.3.

EXAMPLES OF EVIDENCES

- Evidence that contracts with new suppliers and service providers or the procurement guidelines take into account the elements referred to in point 5.1.2 and 5.1.3.
- Comparison between selected contracts and the associated tenders in order 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 EVIDENCES

- 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 impact on the security of the ICT products from suppliers and service providers.
- Evidence from evaluations of suppliers and service providers.

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

- Define responsibilities regarding the maintenance, operation and ownership of assets.
- Make sure that monitoring encompasses periodic reassessment of supplier and service provider compliance, monitoring supplier and service provider release notes, and conducting dark web monitoring.
- Keep track of security incidents related to or caused by third parties.

EXAMPLES OF EVIDENCES

- Records showing that service levels are monitored in accordance with established Service Level Agreements (SLAs).
- 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 the signed contracts with third parties (e.g. contractors, suppliers) are in line with the policy on the security of network and information systems e.g. check the contractual clauses, references to key security relevant roles and responsibilities, requirements for the contractor to report incidents etc.
- 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 in point 5.1.2 of the Annex to the Regulation, consider the following criteria for the use of Open Source Software supply chain (OSS)[29]:
  - risk assessment: before integrating open source libraries, require the supplier or service provider to conduct a thorough risk assessment and communicate the results to the entity in order to understand potential vulnerabilities and their impact on entity's systems;
  - community collaboration: require suppliers or service providers to provide evidence of their engagement with the OSS community for peer reviews and to stay informed about the latest security threats and best practices.
  - updates: ensure that all open source libraries are regularly updated to the latest versions by the supplier or the service provider;
  - licensing: consider the license type (permissive/BSD, copyleft) and their features[30];
  - code reviews: require the supplier or service provider to perform regular code reviews and security testing on open source libraries to identify and address any security issues;
  - software dependencies: require from the supplier or the service provider to provide information on tools to manage dependencies (e.g. Dependabot, Yarn, Gradle, Pip) and ensure that all libraries and their dependencies are secure and up-to-date;

[29] ENISA Secure software engineering initiatives, https://www.enisa.europa.eu/publications/secure-software-engineering-initiatives/@@download/fullReport, accessed 15 October 2024.

[30] Permissive license brings minimal restrictions while copyleft require that any further version of the software is distributed under the same license regime.

    - zero trust: request the supplier or provider to adopt the zero trust model[43] by verifying and authenticating all access requests; and
    - documentation: request the supplier or provider clear documentation and policies for using open source libraries, including guidelines for evaluating, integrating, and maintaining these libraries.
- Consider additional elements for the contract clauses (indicative, non-exhaustive list):
    - clear and complete description of ICT products and ICT services;
    - service level descriptions, including uptime guarantees or target service levels, response times for service issues, 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 case of a cyber incident which present a risk of the ICT product or 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 ICT 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, and provisions on intellectual property.
- Engage with the open source community to stay informed about updates, patches, and best practices for open source software;
- In addition to the elements referred to in point 5.1.5 the entity might consider the following (indicative, non-exhaustive list):
    - country-specific information (e.g. threat assessment from national security services etc.), if available;

  - restrictions or exclusions posed by a relevant national authority, e.g. in 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, the level of transparency and more.
- 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 entity's data within supplier or service provider systems.
- Awareness training should be delivered to the entity's as well as suppliers or service providers' personnel regarding rules of engagement and behaviour 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.
- Make sure that contracts with third parties (e.g. contractors, suppliers) are in line with the policy on the security of network and information systems.

EXAMPLES OF EVIDENCES

- For OSS (indicative, non-exhaustive list)
  - results from risk assessments of the OSS;
  - dependencies' monitoring tools; and
  - documentation.
- Contract clauses which 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 list with additional elements.
- Evidence from awareness trainings.
- Records from crisis management tests (4.3) which demonstrate the participation of relevant personnel of suppliers and service providers.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.19, A.5.20, A.5.21, A.8.30	**BE-CyFun®2023**	IMPORTANT: ID.BE-1.1, ID.GV-1.2, ID.SC-2.1, ID.SC-3.1 ESSENTIAL: ID.SC-1.1, ID.BE-1.2, PR.PT-4.3
NIST CSF v2.0	GV.OC-03, GV.OC-05, GV.SC-01, GV.SC-04, GV.SC-06, GV.SC-05, GV.SC-07, GV.SC-09, GV.SC-10, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	THIRD-PARTIES-1, THIRD-PARTIES-2, CRITICAL-1, CRITICAL-2, CRITICAL-3, WORKFORCE-1, WORKFORCE-3
ETSI EN 319 401	Clauses 7.1, 7.7, ref. to clause 15 of ISO/IEC 27002:2013	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 5**	Cybersecurity Handbook: Part B: 13.1 Self-assessment tool: -
CEN/TS 18026:2024	ISP-02, DEV-08, PM-01, PM-02, PM-04, PM-05	**ES-Royal Decree 311/2022**	Article 2, Article 19, Article 23, Annex II: 4.4.3, 4.4.4, 4.5

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

- Conduct reviews of the registry, at least biannually, to ensure all information is current and accurate.

EXAMPLES OF EVIDENCES

- 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 the end date of the contract as well as the region of each direct supplier and service provider.
- Classify direct suppliers and service providers. 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 e.g cloud providers, data analytic providers, software developers, telecommunication providers etc.
  - Routine: Those with minimal impact on the entity.

EXAMPLES OF EVIDENCES

- List of relevant contracts or service level agreements which are in line with the documented supply chain policy.
- Evidence that the entity has categorized 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 tailors measures accordingly. For instance, “Critical” direct suppliers and service providers receive more attention and customised policies.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.22	**BE-CyFun®2023**	BASIC: ID.GV-4.1, ID.RA-5.1
			IMPORTANT: ID.BE-4.1, ID.RA-5.2, ID.RA-6.1, ID.RM-1.1, ID.RM-2.1, ID.RM-3.1, ID.SC-2.1, ID.SC-3.1, ID.SC-4.1, PR.AC-7.1, DE.CM-6.1, DE.CM-6.2
			ESSENTIAL: ID.RA-5.3, ID.SC-1.1, ID.SC-2.2, ID.SC-3.2, ID.SC-3.3, ID.SC-4.2
NIST CSF v2.0	GV.OC-05, GV.SC-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	THIRD-PARTIES-1, CRITICAL-1
ETSI EN 319 401	-	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 5**	Cybersecurity Handbook: Part B: 13.2, 13.3, 13.4, 13.5, 13.6, 13.7
			Self-assessment tool: 14.2, 14.3, 14.4, 14.5, 14.6, 14.7
CEN/TS 18026:2024	DEV-02, PM-03	**ES-Royal Decree 311/2022**	-

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

6.1 SECURITY IN ACQUISITION OF ICT SERVICES, ICT SYSTEMS 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

- Make cybersecurity fixed part of the purchase process addressing cybersecurity in a separate section.
- Document the secure acquisition of ICT services, systems or products process and describe relevant procedures which support the process.
- Take into account well known standards when developing the process[31].

EXAMPLES OF EVIDENCES

- Tender templates for the acquisition of ICT services, systems or products which address cyber security.
- 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.

GUIDANCE

- The security requirements have to include at least means to detect, monitor and protect against unauthorized changes of software and information.

[31] Additionally to those mentioned in the mapping table at the end of this section, consider also the following:
a) https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services
b) Irish National Cybersecurity Center, Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies), https://www.ncsc.gov.ie/pdfs/Guidelines_on_Cyber_Security_Specifications.pdf, last accessed 14 October 2024.

- Ensure that support contracts cover the system life cycle and obsolescence management requirements, including the date until which the system must be supported and continuous alerting.
- Make sure that tenders request from suppliers or service providers to 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 a penetration testing to identify threats, vulnerabilities, and the potential impact on the entity's operations;
  - potential security tools that need to be already in place e.g. a firewall, an intrusion detection system or a SIEM;
  - specific security mechanism which might be needed to be in place like specific encryption algorithm or a particular access control mechanism (e.g. MFA); and
  - cyber security standards that the entity needs to comply with in order for the ICT service system or product.
- Evaluate the security of systems or products before acquisition.
- Consider criteria for Open Source Software (5.1.2).

EXAMPLES OF EVIDENCES

- Past or on-going tenders for acquiring ICT services, systems or products, address cyber security by referring, as minimum, to the elements outlined in point 6.1.2 of the Annex to the Regulation.
- Comparison between selected contracts and the associated tenders in order 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.

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 secure acquisition of ICT services, systems or products processes and the derived procedures at least annually.
- Review logs or records of all changes made to the secure acquisition of ICT services, systems, or products processes and the derived procedures, including details of the changes, approvals, and implementation dates.
- Align the tenders and contracts with the entity's supply chain security policy (5.1).

EXAMPLES OF EVIDENCES

- Review plans or schedules for the secure acquisition of ICT services, systems or products processes and the derived procedures.
- Minutes from reviews or possible changes made to the ICT services, system or product acquisition processes and the derived procedures, 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 secure acquisition of ICT services, systems or products processes and the derived procedures, including documentation of the review and approval process.
- Incident Response records which confirm whether the entity takes into account significant incidents when reviewing and updating the secure acquisition of ICT services, systems or products process and procedures.

TIPS

GUIDANCE

- Apply the secure acquisition of ICT systems or products 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 in accordance with the entity's supply chain security policy and particularly points 5.1.6 and 5.1.7 of the Annex to the Regulation.
- Additional 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 of the system or the product are discovered;
  - clarify 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
    - 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 entity's data within supplier or service provider systems.

EXAMPLES OF EVIDENCES

- In house projects which take into account the secure acquisition of ICT services, systems or products processes.
- Evidences that points 5.1.6 and 5.1.7 of the Annex to the Regulation are implemented (5.1).
- Tenders with additional to the elements referred to in point 6.1.2 of the Annex to the Regulation.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.21, A.5.23	**BE-CyFun®2023**	BASIC: ID.GV-4.1
			IMPORTANT: ID.RM-1.1, ID.GV-4.2, ID.SC-3.1, ID.SC-4.1, PR.IP-2.1, DE.CM-6.2
			ESSENTIAL: ID.SC-2.2, ID.SC-3.2, ID.SC-4.2, ID.SC-3.3
NIST CSF v2.0	GV.PO-02, GV.SC-06, ID.RA-09, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	THIRD-PARTIES-1, THIRD-PARTIES-2, ARCHITECTURE-4
ETSI EN 319 401	REQ-7.7-01	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 10**	Cybersecurity Handbook: Part B: 13.1, 13.2, 13.4, 13.5
			Self-assessment tool: 14.1, 14.2, 14.4, 14.5
CEN/TS 18026:2024	OIS-04, AM-03, DEV-02, DEV-07, PM-01	**ES-Royal Decree 311/2022**	Article 19, Annex II: 4.1.3, 4.1.5, 4.4.1, 4.4.2

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 well known standards when developing the rules for the secure development of network and information systems.

EXAMPLES OF EVIDENCES

- Documented rules for the secure development of network and information systems which 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;

(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 and development life cycle (SDLC) process should be implemented by all entities, however smaller entities can do with 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).
- Test security by design at various stages of the secure development of SDLC prior to Go-live utilising independent tools and a self-service testing platform throughout SDLC.

EXAMPLES OF EVIDENCES

- 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 to secure development environments, including measures for protecting test data are maintained.
- Evidence of the software testing methods chosen for a particular test scenario and explanation of this.
- Test results of each phase of the SDLC are maintained and are up to date.
- Test results are maintained and approved by management bodies.
- Evidence that a software testing method is chosen at each stage of the software development lifecycle.

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 (point 6.5 of the Annex to the Regulation) and procedures as well as with the secure acquisition of ICT services, systems or products process (point 6.1 of the Annex to the Regulation).
- Hold regular cross organisation unit meetings during all phases of the development life cycle.

EXAMPLES OF EVIDENCES

- Compare the secure development rules with the security testing policy as well as with the secure acquisition of ICT services, systems or products process and check whether the security requirements are set consistently in all these documents.
- Records or minutes from cross organisational units 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 annually.

EXAMPLES OF EVIDENCES

- Documentation that outlines the schedule and the frequency for reviewing secure development rules.
- Documented evidence of the review process of the patch development process, security training for software developments 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 review process of secure development rules.
- Documentation of change requests related to secure development rules, including those initiated 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 separated environments for development purposes, testing purposes and production.
- Ensure the use of results of application assessments in order to regularly enhance developer training and the SDLC process.
- In addition to the regular reviews, the entity should review and, where necessary, update its secure development rules when significant changes to technology or operations or risks or significant incidents.

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.25, A.8.31	**BE-CyFun®2023**	IMPORTANT: ID.GV-1.2, PR.IP-2.1
			ESSENTIAL: PR.DS-7.1, PR.IP-2.2
NIST CSF v2.0	ID.AM-08, PR.PS-06, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ARCHITECTURE-4, THIRD-PARTIES-2
ETSI EN 319 401	REQ-7.7-01, REQ-7.7-02, REQ-7.8-10	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 10**	Cybersecurity Handbook: Part B: 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10, 9.11, 9.12, 9.13, 9.14, 9.15, 9.16
			Self-assessment tool: 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12
CEN/TS 18026:2024	OIS-04, CCM-04, CCM-06, DEV-01, DEV-03, DEV-04, DEV-05, DEV-06	**ES-Royal Decree 311/2022**	Annex II: 5.6.1, 5.6.2, 5.7.1

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[32].
- Maintain operating procedures with details on (indicative, non-exhaustive list):
  - computer start-up and close-down procedures;
  - processing and handling of information;
  - backup;
  - scheduling requirements, including interdependencies with other systems;
  - handling errors or other exceptional conditions;
  - system restart and recovery procedures;
  - 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, 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.
- Ensure compliance with requirements for functions, ports, protocols, and services.
- Monitor and control changes to the configuration settings in accordance with entity's policy on the security of network and information systems as well as topic specific policies and procedures.
- Identify software not authorised to execute on the information systems.

[32] Additionally to those mentioned in the mapping table at the end of this section, consider also the following:
a) ISO/IEC 20000 is the international standard for IT service management. It consists of 17 parts.
b) ITIL (Information Technology Infrastructure Library).
c) IEEE 828, Configuration Management in Systems and Software Engineering.

- Review and update the list of unauthorised software regularly.
- Review and update regularly the list of authorised software.
- Identify software programs authorised to execute on the information system.
- Employ a deny-all, permit-by-exception policy to allow the execution of authorised software.
- Set up procedures for the network service usage to restrict access only to necessary services or applications.
- A secure baseline configuration for development and test environments is managed separately from the operational baseline configuration.
- Identify, document, and approve any deviations from established configuration settings based on defined exceptions on operational requirements.

EXAMPLES OF EVIDENCES

- 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 configuration management plan for asset management, including roles and responsibilities, the assets and configurations that are subject to the plan, the objectives of asset management.
- Documented and approved exceptions to the configuration baseline containing the alternative measures in place to ensure the confidentiality, availability and integrity of the configuration item.
- 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 state-of-the-art hardening guides/best practices and general cyber security principles (e.g., least functionality, least privilege) as a basis to derive the defined security configurations.
- Protect the configuration management plan from unauthorised disclosure and modification.
- 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 configuration management plan containing:
  - roles, responsibilities, and configuration management processes and procedures;
  - a process for identifying configuration items throughout the system development life cycle; and
  - a process for managing the configuration of the configuration items.

EXAMPLES OF EVIDENCES

- Configuration plan.
- Compare the configuration plan with the access control lists.

- Mechanisms e.g. logical and physical access controls, encryption and audit logs are 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 configuration item.

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, where appropriate update, configurations at least monthly to ensure that patches have been applied, the systems run the latest versions of software, the backup has been executed according to the plan and that there are no fatal server/device/disk errors.
- Produce, keep and review regularly change logs regarding security configuration of information systems;
- Review and update the configurations after major changes (e.g software updates) and past incidents.
- Obtain baseline configuration files for key systems and devices to compare against current configurations.

EXAMPLES OF EVIDENCES

- Up to date configuration management plan, review comments and/or change logs.
- 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 configuration changes or deviations from the baseline.
- 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 which confirm whether the entity takes into account incidents related the configurations.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.9	**BE-CyFun®2023**	BASIC: PR.IP-4.1
			IMPORTANT: ID.AM-3.2, PR.IP-1.1
			ESSENTIAL: ID.SC-3.2, PR.DS-1.1, PR.IP-1.2, PR.IP-2.2, DE.CM-7.2
NIST CSF v2.0	PR.PS-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ASSET-3, ASSET-4, ARCHITECTURE-3, ARCHITECTURE-4
ETSI EN 319 401	REQ-6.3-09, REQ-7.7-03	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 2, 10**	Cybersecurity Handbook: Part B: 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.12, 2.15
			Self-assessment tool: 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.12, 3.13
CEN/TS 18026:2024	OPS-21, PSS-03, PSS-04	**ES-Royal Decree 311/2022**	Article 10, Article 20, Article 21, Article 30, Annex II: 4.3.2, 4.3.3

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 well known standards when developing the change management procedures.[33]
- 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 roll-backs; and
  - documentation of the changes and approval of changes.
- The change management procedures may allow different workflows depending on the criticality of the system, scope of the change and urgency (for instance, put in place an "emergency intervention workflow").
- Record for each change the steps of the followed procedure.
- Review and approve changes following the change management procedures, prior to implementing them.
- Implement and test change management procedures, to make sure that changes of networks and information systems are always done following a predefined way.

EXAMPLES OF EVIDENCES

- Documented change management procedures for network and information systems which are based on standards or good practices.
- For each change, a report is available describing the steps and the result of the change.

[33] Additionally to those mentioned in the mapping table at the end of this section, consider also the following:
a) ISO 21500:2021, Project, programme and portfolio management — Context and concepts
b) ISO 21502:2020, Project, programme and portfolio management — Guidance on project management

- A system maintenance procedure that addresses:
  - purpose;
  - scope;
  - roles;
  - responsibilities;
  - management commitment;
  - 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 that changes have to be done in an authenticated, authorised, and non-repudiating manner.
- Test and validate changes before being implemented into 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 (backup images for instance).
- Schedule, perform, document and review records of maintenance and repairs on system components in accordance with supplier’s specifications and/or entity’s requirements.
- Ensure that changes are only allowed with approved tools while their execution has to be documented.
- Restrict the use of maintenance tools to authorised personnel only.

EXAMPLES OF EVIDENCES

- Logs and records of past (new) software installations.
- Evidence that multifactor authentication (MFA) is in place for activating change, repair, and maintenance procedures.
- 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 only approved resources and mandate documentation for each change.
- 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

- Integrate the pullback scenario[34] into the change management procedures.
- Assess the risks from legacy systems and upgrade existing legacy systems to include security mitigating measures in case an appropriate security cannot be achieved.
- Make sure that regular change control procedures which could not be followed due to an emergency change, have to be applied immediately after the emergency change.

EXAMPLES OF EVIDENCES

- Documentation with specific pullback plans.
- Logs and records of past change requests with details on (indicative, non-exhaustive list):
  - details of 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 systems' upgrade which contain risk assessment and 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 annually.
- Make sure that the management procedures cover planned and unplanned changes and the development phase, when applicable.

EXAMPLES OF EVIDENCES

- 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.
- 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.

[34] Also known as 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 that the change does not work as expected.

TIPS

GUIDANCE

- Perform and log changes, maintenance and repairs of network and information systems, with approved and controlled tools.
- Put change management procedures in place according to licensing agreements.
- Upon changes update of the asset inventory (point 12.4 of the Annex to the Regulation) and documentation.
- Inform the customer of significant changes to network and information systems which affect the offered services.
- Ensure availability of 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 there is no information related to the entity contained on 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 connection (OOB) in case that the standard connection does not work.
- Regularly test OOB connections to ensure they function as expected during an outage.
- If an incident, in accordance with Article 23 of the NIS2 Directive, involves post actions, which entail system changes, then notify the competent authorities for these changes in accordance with ENISA guideline on incident reporting or national reporting procedure.

EXAMPLES OF EVIDENCES

- Evidence that multifactor authentication is in place for remote change, repair, and maintenance procedures.
- Logs and records which prove the use of approved tools.
- Evidence that the procedures mention the licencing agreement.
- Documentation of a customer update on significant changes.
- Evidence for previous trainings on change management and system maintenance.
- Evidence of sanitisation procedure.
- 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 which proves the existence of OOB connections.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	6.3, 8.1, A.7.13, A.8.32	**BE-CyFun®2023**	BASIC: ID.AM-1.1, ID.AM-2.1; ID.GV-1.1
			IMPORTANT: ID.AM-1.2, ID.AM-2.2, ID.AM-4.1, ID.GV-1.2, PR.DS-6.1, PR.MA-1.2, PR.MA-1.3, PR.IP-3.1, RS.IM-2.1
			ESSENTIAL: ID.AM-3.3, ID.AM-4.2, PR.IP-2.2, PR.IP-3.2, DE.CM-7.2
NIST CSF v2.0	ID.RA-07, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ASSET-4
ETSI EN 319 401	REQ-7.7-03, REQ-7.7-04	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 15**	Cybersecurity Handbook: Part B: 2.12
			Self-assessment tool: -
CEN/TS 18026:2024	ISP-03, CCM-01, CCM-02, CCM-03, CCM-04, CCM-05, CCM-06	**ES-Royal Decree 311/2022**	Annex II: 4.3.5

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 well known standards when developing the testing policy[32].
- Establish and maintain a testing program appropriate to entity's size, complexity, and maturity[35].

EXAMPLES OF EVIDENCES

- Documented security testing and procedures which are 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.

[35] Cyber fundamentals, ID.RA-1, Centre for Cyber Security Belgium, accessible at: https://ccb.belgium.be/sites/default/files/cyberfundamentals/CYFUN_IMPORTANT_EN_20230301.pdf

GUIDANCE

- Make sure that network and information systems are tested at set up, after infrastructure or application upgrades or modifications that the entity determines are significant, or after maintenance.
- Consider a range of security tests, e.g. vulnerability assessments, penetration testing, code review, ethical-hacking, cyber-attack simulations or cyber response exercises etc.
- Entity wide 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 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 cyber security risk assessments (section 2.1, and in particular in point 2.1.2 of this document).
- Assess, follow up and remediate findings at least in the case of medium to very high criticality with respect to the confidentiality, integrity, authenticity or availability of the service provided.
- The assessment of criticality and mitigating actions for each finding are documented.

EXAMPLES OF EVIDENCES

- Documented security testing policy and procedures which include the elements referred to in point 6.5.2 (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, 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 annually.

EXAMPLES OF EVIDENCES

- 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, test report templates.

TIPS

GUIDANCE

- Determine the auditable security events that are adequate to support investigations of security incidents.
- Implement tools for automated testing, such as code analysis tools or vulnerability scanners.
- Ensure the policy is approved, communicated to and acknowledged by relevant personnel and third parties.
- Ensure that the development and testing environment(s) 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 EVIDENCES

- Additionally to the elements referred to in point 6.5.2 (c) of the Annex to the Regulation documented policy which at least include (indicative, non-exhaustive list):
  - approved parties (internal or third);
  - confidentiality levels for assessment; and
  - test results and the objectives security assessments and tests.
- Relevant staff is aware of the security testing procedures and tools.
- Audit requirements are approved by the management bodies.
- A list of tools used for security testing, including their purpose and how they are maintained and updated.
- Valid licenses for commercial testing tools or subscriptions to security services.
- Records showing updates to the security policy and procedures based on lessons learnt and new threats.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.29, A.8.33, A.8.34	**BE-CyFun®2023**	IMPORTANT: ID.BE-5.1, ID.SC-4.1, PR.IP-3.1, PR.P-4.2, PR.IP-7.3, PR.MA-1.3, RS.CO-1.1, RS.IM-1.2, RC.IM-1.1 ESSENTIAL: ID.RA-1.3, ID.SC-3.2, ID.SC-4.2, PR.DS-7.1, PR.IP-2.2, PR.IP-3.2, DE.DP-5.2
NIST CSF v2.0	ID.RA-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	THREAT-1, THIRD-PARTIES-2
ETSI EN 319 401	REQ-7.8-10, REQ-7.8-14, 14A, REQ-7.8-15	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 14**	Cybersecurity Handbook: Part B: 14.4, 14.5, 9.13, 9.14 Self-assessment tool: 15.6, 15.7, 15.8, 15.9, 10.10, 10.11
CEN/TS 18026:2024	ISP-02, OPS-19, DEV-01, DEV-04, DEV-06	**ES-Royal Decree 311/2022**	Annex II: 4.5

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.[32,36]
- Actions may vary, depending on the system (e.g. mandatory patching for exposed systems (e.g. internet-connected devices like firewalls and routers) and limited patching for isolated or legacy systems).
- Establish a process, in combination with the asset inventory, to be 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.
- Deploy vulnerability management technologies to identify unpatched and misconfigured software.
- Define your relevant security information sources considering your assets and continuously monitor them for patches 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.
- Apply patches after approval or testing on an isolated environment, following the change management procedure.

EXAMPLES OF EVIDENCES

- 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 (12.4) is updated after a new security patch is announced accompanied by the time plan to apply 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.

[36] Additionally to those mentioned in the mapping table at the end of this section, consider also 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, last accessed 15 October 2024.

- Detailed audit trails showing the steps taken from patch identification to deployment.
- Checks for latest patches.
- Approved documented actions applying patches.
- Records of changes logged, reviewed, and approved.
- Evidence for vendor verification mechanisms e.g digital certificates, digital signatures etc.
- Reports from internal and external audits evaluating the effectiveness of the patch management processes.

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

- Take effort, proportionate to entity's size and importance, to ensure that security patches don't introduce additional vulnerabilities or instabilities.
- If patching is not feasible, consider compensating measures like hardening, intrusion detection systems, network segmentation, access control and monitoring.

EXAMPLES OF EVIDENCES

- Evidence from patch prioritisation e.g emphasis is given on patches assessed as critical.
- Evidence that residual risks resulting from non patching are listed and mitigated.
- Incident reports related to unpatched vulnerabilities in order to check the effectiveness of the mitigation measures during entity's response.
- Logs of changes made to systems, including patches applied, rollback procedures, and any issues encountered.
- Documented decisions for non patching accompanied by relevant compensating measures.

TIPS

GUIDANCE

- Inform customers in advance in case of planned inaccessibility to the service.
- Patch management procedures indicating scope, roles & 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, in case that patching does not work, to ensure that the system reverts to a safe previous state.
- Remove unsupported hardware and software from the network in a reasonable and accepted timeline in line with the entity's risk assessment.
- Include patch and update requirements in the supply chain policy (5.1) as well as in the contracts, bid evaluation and selection criteria for new ICT services, systems or products (secure acquisition of ICT services, systems or products, 6.1), also considering the system life span.

EXAMPLES OF EVIDENCES

- Evidence of communications e.g. sms, emails, announcement, posts at media etc. with the customers related to inaccessibility of the service.
- 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 for latest patches for evidence of who performed each step and when as well as 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, documented evaluation and selection criteria for new systems which consider the patch management requirements as well as the system life span.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.31, A.8.32	**BE-CyFun®2023**	BASIC: PR.MA-1.1
			IMPORTANT: PR.MA-1.2, PR.IP-1.1
			ESSENTIAL: ID.SC-3.2, PR.MA-1.7
NIST CSF v2.0	PR.PS-02, DE.CM-09, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ASSET-4, THREAT-1
ETSI EN 319 401	REQ-7.7-09	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 10**	Cybersecurity Handbook: Part B: 2.8
			Self-assessment tool: 3.5, 3.6, 15.4
CEN/TS 18026:2024	CCM-03, CCM-04, CCM-05, OPS-18	**ES-Royal Decree 311/2022**	Annex II: 4.3.2

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 developing the supply chain policy[37].

EXAMPLES OF EVIDENCES

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

[37] Additionally to those mentioned in the mapping table at the end of this section, consider also the following:
a) NIST Special Publication NIST SP 800-215, Guide to a Secure Enterprise Network Landscape, https://csrc.nist.gov/pubs/sp/800/215/final, accessed 15 October 2024.
b) ISO/IEC 27033 series of standards on network security.

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;

(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

- Define roles and responsibilities as well as timelines for the transition towards 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 STARTTLS, DANE, DMARC, DKIM and SPF[38]
  - internal spam/scam/virus filtering; and
  - URL rewriting.
- Consider DNS SEC[39] for DNS.
- Consider BGP[40] for internet routing.

EXAMPLES OF EVIDENCES

- Up-to-date network diagrams, including the Out-Of-Band (OOB) connections.
- Firewall(s).
- Configuration files and rulesets for firewalls and routers, showing how traffic is filtered and managed.

[38] https://ec.europa.eu/internet-standards/email.html
a)

[39] a) Secure Domain Name System (DNS) Deployment Guide http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf, accessed 15 October 2024.
b) DNSSEC HOWTO, a tutorial in disguise Olaf Kolkman, https://www.dns-school.org/Documentation/dnssec_howto.pdf, accessed 15 October 2024.

[40] ENISA, 7 Steps to shore up the Border Gateway Protocol (BGP), https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp, accessed 15 October 2024.

- Configuration files for switches, including Virtual Local Access Network (VLAN) settings and access control lists (ACLs).
- Documentation of ACLs implemented on network devices to control traffic flow.
- Documented correct usage of mobile devices and other remote-accesses (e.g. teleworking, OOB connections).
- Evidence of controls over privileged accounts, including logs and policies.
- Access logs to confirm that only authorised personnel are making changes and conducting reviews of the network security rules.
- Transition towards latest generation network layer communication protocols implementation plan.

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 network security measures' review depends on the entity's risk assessment as a general rule the entity might (indicative, non-exhaustive list):
  - continuously monitoring the networks for real time threats;
  - weekly perform scans for new vulnerabilities;
  - update the rules of the firewall and other tools on a monthly basis; and
  - assess thoroughly 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.

EXAMPLES OF EVIDENCES

- 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 Security Information and Event Management (SIEM) systems showing aggregated and analysed security events.
- VPN and Remote Access Logs showing remote, including OOB connections, access attempts, successful connections, and any anomalies.
- Evidence of Network Access Control (NAC) 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 access control list (ACL) reviews.
- Documentation showing regular reviews of user and administrative access to network devices.
- Audit logs from network security devices (e.g., firewalls, IDS/IPS[41]) 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.

[41] Intrusion detection/prevention systems

- 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 and other remote-accesses.

EXAMPLES OF EVIDENCES

- The correct usage of mobile devices and other remote-accesses (e.g. teleworking, VPN) has been communicated to the personnel.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.16, A.8.20	**BE-CyFun®2023**	BASIC: ID.RA-1.1, PR.AC-2.1, PR.AC-3.1, PR.AC-3.2, PR.AC-5.1, PR.AC-5.2, DE.CM-1.1, DE.CM-3.1
			IMPORTANT: PR.AC-2.2, PR.AC-3.3, PR.AC-5.3, PR.AC-5.4, PR.AT-1.2, DE.CM-1.2, DE.CM-3.2
			ESSENTIAL: ID.BE-1.2, PR.AC-2.4, PR.AC-5.5, DE.CM-1.3
NIST CSF v2.0	DE.CM-01, PR.IR-01, PR.PS-05, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ACCESS-1, ACCESS-2, ARCHITECTURE-1, ARCHITECTURE-2
ETSI EN 319 401	REQ-7.8	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 13, 17**	Cybersecurity Handbook: Part B: 6.1, 6.2, 6.3, 6.8, 6.9, 6.10, 6.11, 6.12, 6.13, 6.14, 6.15, 6.16, 6.17, 6.18, 6.19, 6.20, 6.21, 6.22, 6.23
			Self-assessment tool: 7.1, 7.2, 7.3, 7.8, 7.9, 7.11, 7.12, 7.13, 7.14, 7.16, 7.17, 7.18, 7.19, 7.20, 7.21
CEN/TS 18026:2024	PS-04, CS-01, CS-02, CS-03, CS-06, CS-07, CS-08, PSS-02	**ES-Royal Decree 311/2022**	Article 9, Annex II: 5.4.1, 5.4.2, 5.4.3

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[42], [43].

EXAMPLES OF EVIDENCES

- Documented network segmentation rules which are 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[44, 45]

- Make sure that the segments are in line with the results of the risk assessment (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.
- Implement subnetworks for publicly accessible system components that are physically and/or logically separated from internal organisational networks.
- Determine the degree of physical separation of system components from physically distinct components:
  - in separate racks in the same room;

[42] Additionally to those mentioned in the mapping table at the end of this section, consider also the following:
b) NIST Special Publication NIST SP 800-215, Guide to a Secure Enterprise Network Landscape, https://csrc.nist.gov/pubs/sp/800/215/final, accessed 15 October 2024.
c) ISO/IEC 27033 series of standards on network security.

[43] Zero trust model proposed by NIST and it assumes that no part of the network is trusted (NIST Special Publication NIST SP 800-215).

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

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

    - in separate rooms for the components with high criticality; and
    - to more significant geographical separation of the components with high criticality.
- Implement separate network addresses (i.e., different subnets) to connect to systems in different security domains.
- Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.
- Isolate information security tools, mechanisms, and support components from other internal information system components 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 purposes of access control and auditing.
- Implement a managed interface for each external telecommunication service.

EXAMPLES OF EVIDENCES

- 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[46], internal networks, guest networks).
- Verify that the diagrams align with business functions and risk profiles.
- Documented criteria for creating and maintaining different network zones.
- Virtual Local Access Network (VLAN) configurations on network switches and routers.
- VLANs correspond to different security zones and business functions.
- Measures (e.g., IDS/IPS[41], monitoring systems) tailored to each network zone.
- Configurations of network devices (e.g., routers, switches, firewalls) for proper segmentation settings.
- Configuration settings match documented segmentation rules and diagrams.
- Segregation of duties control matrix.
- Access Control Lists (ACLs) and firewall configurations

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 biannually.

EXAMPLES OF EVIDENCES

- Reports from recent penetration tests and vulnerability scans.
- Network segmentation rules' review plans or schedules.
- Logs or records confirming that the reviews have been conducted according to the schedule.
- Change management documentation for network segmentation changes, in line with risk assessment results and business needs.

[46] A perimeter network, also known as a demilitarized 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.

- 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 are 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 are conducted periodically and after major changes or incidents, and their findings lead to rule reviews.

TIPS

GUIDANCE

- Limit the data traffic between the different segments to the operationally required extent by means of data flow control, e.g. 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 like:
    - gateways;
    - routers;
    - firewalls;
    - guards;
    - network-based malicious code analysis;
    - virtualization systems; and
    - encrypted tunnels.
- Prevent discovery of specific system components composing a managed interface.
- Exceptions are monitored

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.22	**BE-CyFun®2023**	BASIC: PR.AC-3.1, PR.AC-5.2
			IMPORTANT: PR.AC-5.3, PR.AC-5.4, PR.IP-4.3
			ESSENTIAL: ID.BE-5.2, PR.DS-7.1, PR.IP-3.2, PR.IP-4.5
NIST CSF v2.0	PR.IR-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ARCHITECTURE-1, ARCHITECTURE-2
ETSI EN 319 401	REQ-7.8-02	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 13**	Cybersecurity Handbook: Part B: 6.4, 6.5, 6.6, 6.7, 6.15
			Self-assessment tool: 7.4, 7.5, 7.6, 7.7, 7.15
CEN/TS 18026:2024	IAM-09, CS-02, CS-04, CS-05	**ES-Royal Decree 311/2022**	Annex II: 5.4.4

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 malicious and unauthorised software detection and protection mechanisms 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, removable media, or inserted through the exploitation of system vulnerabilities.
- Configure malicious code protection mechanisms to perform periodic scans of the system regularly and real-time scans of files from external sources as the files are downloaded, opened, or executed.
- Disinfect and quarantine infected files.
- Apply application whitelisting and monitor unauthorised activities and system behaviour.
- Make sure that the malicious and unauthorised protection mechanisms are centrally managed.
- Make sure that there are mechanisms which 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 as well as patch management procedures of the entity.
- Address issues related to false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

- Align malicious and unauthorised detection and repair software monitoring and logging rules with entity's monitoring and logging tools and procedures (3.2) as well as with entity's access control (11.1) and asset handling policy.

EXAMPLES OF EVIDENCES

- Endpoint protection systems (EPS) across the network.
- Malware detection systems are present, and up to date.
- Tools for monitoring unauthorised software is in place and up to date.
- Firewall configurations, intrusion detection/prevention systems (IDS/IPS), and secure web gateways contain 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 are up to date.
- Documented description of centrally management tools.
- Records of recent updates malicious and unauthorised detection and repair software which show that they are regularly patched and updated to protect against known vulnerabilities.
- Records of periodical scans.
- Monitoring and logging of network and information systems, at discrete intervals to identify malicious code and unauthorized code execution.
- Logs for blocked or detected threats.
- Record and maintain logs including:
    - user activities;
    - exceptions; and
    - information security incidents.
- Documented spam protection mechanism.
- Determine the level of logs monitoring required by a risk assessment.

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 execution 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 filtering are (indicative, non-exhaustive list):
    - content filtering;
    - blocklist filtering;
    - antivirus filtering;
    - phishing filters; and

- machine learning filters.

EXAMPLES OF EVIDENCES

- Documented alternative countermeasures such as:
  - Securing of 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 which confirm that administrative privileges are controlled and monitored.
- Logs from email filters.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.32, A.8.7	**BE-CyFun®2023**	BASIC: ID.AM-2.1, ID.RA-1.1, PR.PT-4.1, DE.CM-4.1
			IMPORTANT: ID.AM-2.4, DE.CM-5.1
			ESSENTIAL: ID.AM-2.5, PR.MA-1.6, PR.PT-2.3, DE.CM-4.2, DE.DP-5.2
NIST CSF v2.0	DE.CM-01, DE.CM-09, PR.PS-05, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ARCHITECTURE-2, ARCHITECTURE-3
ETSI EN 319 401	REQ-7.7-05	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 13, 17**	Cybersecurity Handbook: Part B: 6.9, 6.10, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7,10
			Self-assessment tool: 7.9, 7.10, 7.11, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10
CEN/TS 18026:2024	OPS-04, OPS-05, CS-03	**ES-Royal Decree 311/2022**	Article 24, Annex II: 4.3.6

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 e.g CVSS, EPSS, SANS vulnerability assessment framework etc.

EXAMPLES OF EVIDENCES

- 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

- Address without undue delay vulnerabilities assigned to the highest classification (e.g. ”critical” in CVSS) or equivalent (e.g. as defined by the national CSIRT). Accepting the risk of such vulnerabilities, and not addressing them, is not advisable, where possible.
- Share information obtained from the technical vulnerability scans with designated personnel throughout the entity and authorities to help eliminate similar vulnerabilities in other information systems.
- Disclose not yet known vulnerabilities to designated CSIRT according to national Coordinated Vulnerability Disclosure (CVD) policies, where applicable.
- Identify a single point of contact and communication channels for network and information security related issues with suppliers and service providers.

EXAMPLES OF EVIDENCES

- Logs of a vulnerability assessed as critical to check if it was addressed.
- Licenses 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 logs for records of detected vulnerabilities and related alerts from monitoring channels.
- Reports from third-party security assessments or penetration tests.
- Evidence of addressed findings from these assessments for vulnerabilities assessed as critical.
- Records from a vulnerability disclosed, if any, according to the national CVD policy.
- Interview the single point of contact and communication channels for information security related issues with suppliers and service providers.

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

- Define and establish the roles and responsibilities associated with vulnerability management.

EXAMPLES OF EVIDENCES

- Records showing timelines and responsible employees for each remediation effort as well as verification of fixes.

- Records or logs of past vulnerability mitigation plans or schedules.
- Records of a vulnerability which was not addressed and the relevant justification.

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 technical vulnerability monitoring channels' information at least biannually.
- Consider inventorying sources likely to report technical vulnerabilities in the identified components and distribute updates (software publisher websites, CERT website, ENISA website)[47].

EXAMPLES OF EVIDENCES

- List of technical vulnerabilities' monitoring channels, including suppliers and service providers' single point of contacts.
- Records of past and plans for future technical vulnerability channels' reviews.
- Subscriptions to relevant vulnerability notification services, mailing lists, and alert systems (e.g., CERT, vendor advisories, 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).

TIPS

GUIDANCE

- Create and maintain procedures for identifying, assessing, prioritising, and remediating vulnerabilities.
- Make sure that suppliers and service providers report vulnerabilities of their systems or products or services that present a risk to the security of the network and information systems of the entity (supply chain policy, 5.1.4).
- Perform vulnerability scans, and record evidence of the results of the scans, when significant incidents or significant changes to operations or risks occur.
- Review and, where appropriate, update the channels of monitoring vulnerability information when significant incidents or significant changes to operations or risks occur.

EXAMPLES OF EVIDENCES

- Documented procedures for identifying, assessing, prioritising, and remediating vulnerabilities.
- Contracts with suppliers and service providers which require technical vulnerability reporting, handling and disclosure.
- Evidences from supplier and service providers vulnerability related communications or reports
- Records of ad-hoc scans performed in response to significant incidents or changes to the infrastructure, including the dates and reasons for these scans.

[47] Cyber fundamentals, PR.IP-12, Centre for Cyber Security Belgium, accessible at: https://ccb.belgium.be/sites/default/files/cyberfundamentals/CYFUN_IMPORTANT_EN_20230301.pdf

- Change management logs to verify that vulnerability scans are conducted following significant incident 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.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.8[48]	**BE-CyFun®2023**	BASIC: ID.RA-1.1 IMPORTANT: ID.RA-1.2, ID.RA-2.1, DE.CM-8.1, DE.CM-8.2, DE.DP-4.1, RS.AN-5.1 ESSENTIAL: ID.AE-3.3, DE.DP-5.2, RS.AN-5.2
NIST CSF v2.0	ID.RA-01, ID.RA-02, ID.RA-04, ID.RA-05, ID.RA-06, PR.PS-02, PR.PS-03, ID.RA-08, ID.RA-06, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	THREAT-1
ETSI EN 319 401	REQ-7.8-13, REQ-7.8-13A, REQ-7.9-10, REQ-7.9-11	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 14**	Cybersecurity Handbook: Part B: 14.1, 14.2, 14.3 Self-assessment tool: 15.1, 15.3, 15.4, 15.5
CEN/TS 18026:2024	OIS-03, OPS-17, OPS-18, OPS-19, OPS-20, OPS-21, DEV-06	**ES-Royal Decree 311/2022**	Article 8, Article 10, Article 21, Article 34, Annex II: 4.7.3, 5.8.2

[48] ISO/IEC 29147 provides detailed information on receiving vulnerability reports. ISO/IEC 30111 provides detailed information about handling and resolving reported vulnerabilities.

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

7.1.1. 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 well known standards when developing the policy and procedures for assessing the efficient implementation of the measures.[49]
- Implement a policy for assessing the effectiveness of implementation of measures which is proportionate to the risk posture of the entity in line with the risk assessment.

EXAMPLES OF EVIDENCES

- Documented policy and procedures for effectiveness assessments which is based on standards.

7.1.2. 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):
  - self-assessment;
  - benchmarking against a measure's checklist or a standard;
  - vulnerability assessment;

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

  - 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 case of externals, confidentiality and non-disclosure terms should be included in the contract.
  - Internal employees should be suitably trained, and the entity should consider their objectivity and impartiality. The entity should pay particular attention to the elements of point 2.3. of the Annex to the Regulation concerning impartiality of the employees. For instance, they should not come from the department or division whose systems are being inspected or should not have been involved in developing the code and in installing or operating the system being audited for this purpose.
- Define key performance indicators (KPIs) to measure the effectiveness of measures including notable examples like (indicative, non-exhaustive list)[50]:
  - the cost of implementation and maintenance e.g. CAPEX/OPEX.
  - the number of employees who have attended cyber security trainings;
  - the number of vulnerabilities detected;
  - time to remediation;
  - incident response times; and
  - number of non-compliances (consider the elements of point 2.2. of the Annex to the Regulation concerning the 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 under point 7.2.1 (a) of the Annex of 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, incident response plans);
  - annually assess the overall effectiveness of all measures;
  - measure the effectiveness of measures related to a specific incident following that incident; and
  - measure the effectiveness of measures related to a specific systems or one of its components following significant changes to this system or this component.

EXAMPLES OF EVIDENCES

- 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 (point 2.3.3. of the Annex to the Regulation concerning the compliance monitoring).
- Documented objectives and KPIs for the implementation of the measures.
- Documented analysis and evaluation of the results from the evaluations.

[50] ENISA's cyber security investment reports offer a good reference for measuring effectiveness of measures e.g. NIS Investments report 2023, https://www.enisa.europa.eu/publications/nis-investments-2023, last accessed 19 October 2024.

- Logs or records from previous effectiveness assessments.
- Plans or schedules for future effectiveness assessments.
- Documented roles and responsibilities.

7.1.3. 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.
- Update the policy and procedures based on findings from security tests (Annex to the Regulation, point 6.5) and the independent review of policy on the security of the network and information systems (Annex to the Regulation, point 2.3), if applicable.
- Take into account the results of the assessment and consider them when identifying and prioritising appropriate risk treatment options and measures (point 2.1.3 of the Annex of the Regulation).

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	6.2, 9.1, 9.3	**BE-CyFun®2023**	BASIC: RS.IM-1.1
			IMPORTANT: PR.IP-7.1, PR.IP-8.1, PR.IP-8.2, PR.IP-9.1, DE.DP-3.1, RS.IM-1.2, RC.IM-1.1
			ESSENTIAL: PR.IP-7.2, PR.IP-7.3, PR.IP-9.2
NIST CSF v2.0	ID.IM-03, GV.RM-06, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	CRITICAL-2, RISK-4, RISK-5, Management activities
ETSI EN 319 401	Clause 5, ref. to ISO/IEC 27005:2011	**EL – Ministerial decision 1027/2019 Article 4 - paragraph 14**	Cybersecurity Handbook: Part B: 14.1, 14.2, 14.3, 14.4, 14.5
			Self assessment tool: 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7, 15.8, 15.9
CEN/TS 18026:2024	ISP-02, OPS-20, CO-04	**ES-Royal Decree 311/2022**	Article 31, Article 32, ANNEX III - Security audit

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 programs:
  - Use various formats, such as workshops, webinars, and e-learning modules.
  - Use multiple communication channels (emails, newsletters, intranet) to keep employees informed about cybersecurity updates, threats, and cyber hygiene practices for users.

EXAMPLES OF EVIDENCES

- Awareness raising program, e.g. a comprehensive outline of the program, detailing the objectives, content, frequency, syllabus, and schedule of the program.

8.1.2. The relevant entities shall offer to all employees, including members of management bodies, 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 for users (indicative, non-exhaustive list):
  - clear desk and screen policy,
  - use of passwords and other authentication means,
  - event reporting,
  - safe email use and web browsing,
  - protection from phishing and social engineering,
  - secure use of mobile devices,
  - secure connection practices,
  - backup practices,
  - secure teleworking practices and more.
- Include in the programme the following topics (indicative, non-exhaustive list):
  - Train personnel to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

  - Train personnel to be aware of causes for unintentional data exposure. Example topics include erroneous delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.
  - Train personnel on the dangers of connecting to, and transmitting data over, insecure networks for 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 on understanding malicious and unauthorised software, on the importance of malicious software detection and on the risks and consequences of using unauthorised software.
- Offer to employees contact points and resources for additional advice.
- To implement the awareness raising program, consult available sources, such as ENISA's AR-in-a-Box.[51] and the Cybersecurity Skills Academy[52].

EXAMPLES OF EVIDENCES

- Awareness raising program, i.e. a comprehensive outline of the program, detailing the objectives, content, frequency, syllabus, schedule of the program.
- Copies of the awareness raising materials distributed to employees, including handouts, e-mails, presentations, and online modules.
- Logs, sign-in sheet, certificates of completion or acknowledgements given to employees upon completing the program, that show which employees followed the awareness raising program.

8.1.3. The awareness raising program shall be tested in terms of effectiveness, 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.
- Test the effectiveness of the awareness raising program, e.g. by using quizzes.
- Review and update the awareness raising program at least annually.

EXAMPLES OF EVIDENCES

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

[51] https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising-in-a-box

[52] 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, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A207%3AFIN, last accessed 5.10.2024.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	7.3, A.6.3, A.8.7	**BE-CyFun®2023**	BASIC: PR.AT-1.1
			IMPORTANT: PR.AT-1.2
			ESSENTIAL: PR.AT-1.3
NIST CSF v2.0	PR.AT-01, PR.AT-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	WORKFORCE-2, WORKFORCE-3, WORKFORCE-4, PROGRAM-2
ETSI EN 319 401	REQ-7.2-02, REQ-7.2-03, REQ-7.2-04	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 16**	Cybersecurity Handbook: Part B: 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12, 10.13, 10.14, 10.15, 12.1
			Self-assessment tool: 11.1, 11.5, 11.6, 13.1
CEN/TS 18026:2024	HR-04, DOC-01	**ES-Royal Decree 311/2022**	Annex II: 5.2.3

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 the European Cybersecurity Skills Framework (ECSF)[53].

EXAMPLES OF EVIDENCES

- A comprehensive outline of the training program, 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.
- Consider various training methods, such as online courses, workshops, hands-on labs, and simulations
- Consider various types of trainings, such as courses, certifications, or attending security conferences or webinars.
- Examples of trainings may include secure system administration courses for IT professionals, OWASP® awareness and prevention trainings for web application developers, and advanced social engineering awareness training for high-profile roles.

EXAMPLES OF EVIDENCES

[53] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework, last accessed 5.10.2024.

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

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 to the programme may include (indicative, non-exhaustive list):
  - Train personnel on authentication best practices, such as MFA, password creation, and credential management.
  - Train personnel on how to identify and properly store, transfer, archive, and destroy sensitive data.
  - Train personnel to recognize a potential incident, such as unusual email attachments, unexpected system behaviour, and suspicious network traffic.
  - Train staff on 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.
  - Provide regular updates on the latest cyber threats.
- Test the security knowledge of employees to make sure that they have sufficient and up-to-date security knowledge.

EXAMPLES OF EVIDENCES

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

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 EVIDENCES

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

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 trainings periodically.
- Review and update the training program at least annually.

EXAMPLES OF EVIDENCES

- Logs, sign-in sheets, certificates of completion or acknowledgements given to employees upon completing the training, that show which employees attended the training sessions.
- Training materials distributed to employees, including handouts, presentations, and online modules.
- Updates showing that the training program 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.

TIPS

GUIDANCE

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	7.2, A.6.3	**BE-CyFun®2023**	BASIC: PR.AT-1.1
			IMPORTANT: PR.AT-1.2, PR.AT-5.1, RC.IM-1.1
			ESSENTIAL: PR.AT-1.3
NIST CSF v2.0	PR.AT-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	WORKFORCE-1, WORKFORCE-2, WORKFORCE-3, WORKFORCE-4
ETSI EN 319 401	REQ-7.2-03	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 16**	Cybersecurity Handbook: Part B: 12.1, 12.2, 12.3, 12.4, 12.5
			Self-assessment tool: 13.1, 13.2, 13.3, 13.4, 13.5, 13.6
CEN/TS 18026:2024	HR-04, PM-01	**ES-Royal Decree 311/2022**	Annex II: 5.2.4

9. CRYPTOGRAPHY

9.1.1. 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.

EXAMPLES OF EVIDENCES

- Documented policy on cryptography and procedures related to cryptography.

9.1.2. The policy and procedures referred to in point 9.1.1. 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.

GUIDANCE

- Ensure that the policy and procedures cover cryptographic mechanisms, such as digital signatures and hashes, to:
  - protect the confidentiality and integrity of data in transit and at rest;
  - detect unauthorized changes to data at rest marked as critical; and
  - secure disposal of the data after their 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, key management).
- Enforce encryption on electronic media which contain confidential/sensitive information.
- Ensure confidentiality and integrity of the data with cryptographic mechanisms, when, for example (indicative, non-exhaustive list):
  - sharing information;
  - scanning;
  - 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, e.g. by escrowing of encryption keys.
- Produce, control, and distribute symmetric and asymmetric cryptographic keys using key management technology and processes.
- Use 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 for key management activities like:
  - key generation;
  - keys destruction; and
  - key archiving;
- 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[54]. Key features of this approach are:
  - Flexibility in algorithm selection.
  - Modular design of the architecture where cryptographic components can be changed or updated independently without impacting the entire system.
  - Regular updates and patching.
  - Compliance with the legislative frameworks as well as governance of the use of the cryptography within the entity's networks and information systems.
  - Future proofing by considering quantum cryptographic algorithms.

EXAMPLES OF EVIDENCES

- Documented policy on cryptography which is in line with relevant regulations and state of the art standards.
- Documented guidelines for encryption.

[54] Crypto-agility, or cryptographic 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.

- Acceptable, in line with the state of the art, encryption algorithms, key lengths, protocols[55] or family of protocols[56].
- Safeguards to protect the secrecy of secret (private) key(s) are in place
- Evidence for the existence of cryptographic mechanisms which support in ensuring confidentiality and integrity of the data at rest as well as 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.

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

EXAMPLES OF EVIDENCES

- 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.

[55] 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 SSL/TLS and SSH.

[56] A family of cryptographic protocols refers to 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.

- Evidence that the entity remains up to date with the last developments in cryptography (e.g. member of cryptographic bodies or consortia (e.g., IETF, Cryptographic Research Groups), 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.

EXAMPLES OF EVIDENCES

- Records of training programs related to cryptography for employees.
- Employees are aware of the confidentiality and integrity of the data and communications and procedures and what it implies for their work.
- Employees handling sensitive information are aware of and understand the cryptography policies and procedures.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.31, A.8.24	**BE-CyFun®2023**	IMPORTANT: PR.DS-6.1 ESSENTIAL: PR.AC-3.4, PR.DS-8.1
NIST CSF v2.0	PR.DS-01, PR.DS-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ARCHITECTURE-5
ETSI EN 319 401	Clause 7.5, ref. to clause 10 of ISO/IEC 27002:2013	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 11**	Cybersecurity Handbook: Part B: 5.5, 6.22, 9.10, 9.16, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.8 Self-assessment tool: 6.7, 10.7, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7
CEN/TS 18026:2024	ISP-02, CKM-01, CKM-02, CKM-03, CKM-04	**ES-Royal Decree 311/2022**	Annex II: 4.3.10, 5.5.2

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, demonstrate 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.

EXAMPLES OF EVIDENCES

- List of employees 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 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 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.
- Certifications or attestations from recognized bodies confirming adherence to security standards and policies.

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).
- 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).

- Provide 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 (Annex to the Regulation, point 8.2).
- Conduct thorough reference checks to verify the candidate’s previous experience and performance in similar roles.
- Implement vetting procedures, including background checks (Annex to the Regulation, point 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 that include security experts to assess the candidate’s technical and behavioural competencies.

EXAMPLES OF EVIDENCES

- Training and awareness raising material such as videos, slides, emails, newsletters, posters and intranet announcements.
- Documented records 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, policy on the security of network and information systems, terms and conditions, code of conduct, other documentation confirming that all users have understood and are following the standard cyber hygiene practices for users(signed employment contracts, any proof of informing employees about their responsibilities having to do with network and information security).
- Records of security training sessions provided to employees, including attendance logs and training schedules.
- Evidence, e.g attendance certificates, that suppliers and service providers receive security training relevant to their roles.
- Mechanisms for hiring qualified personnel (e.g. reference check, validation of certifications, written tests) are in place.

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 EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	7.1, 7.2, A.6.2, A.6.3	**BE-CyFun®2023**	BASIC: ID.GV-1.1, PR.AC-1.1, PR.AC-4.3, PR.IP-11.1
			IMPORTANT: ID.AM-6.1, ID.GV-1.2, ID.SC-3.1, PR.AC-2.2, PR.AC-4.6, PR.IP-11.2, DE.CM-6.2
			ESSENTIAL: ID.BE-1.2, ID.SC-3.2, ID.SC-3.3
NIST CSF v2.0	PR.AT-02, GV.RR-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	WORKFORCE-1, WORKFORCE-2, WORKFORCE-3, THIRD-PARTIES-1, THIRD-PARTIES-2, Management activities
ETSI EN 319 401	REQ-7.2	**EL – Ministerial decision 1027/2019 -**	
CEN/TS 18026:2024	HR-01, HR-02, HR-03	**ES-Royal Decree 311/2022**	Article 15, Annex II: 5.2

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 10.2.2(a).
- Perform verification of background of employees, and where applicable of direct suppliers and service providers in accordance with point 5.1.4.

EXAMPLES OF EVIDENCES

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

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

- Define criteria for roles, responsibilities and authorities which 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 involved with procurement and vendor management.
  - Roles that grant access to physical assets or responsible for physical security.
- Define criteria and limitations for verification of background (e.g. who is eligible to screen people and how, when and why verification reviews are carried out).
- Include in the verification of background, a check of the criminal records of the person concerned with regards to offences which would be relevant for a specific position.
- Collect and handle information on job candidates taking into consideration any applicable law, regulations, and ethics, including the protection of personal data. This may include the collection of professional references.
- Include screening requirements in the contractual agreements between the entity and the direct suppliers and service providers, in case of personnel contracted with an external supplier.
- Periodically repeat verification in order to confirm ongoing suitability of personnel, depending on the criticality of a person's role, responsibilities and authorities.

EXAMPLES OF EVIDENCES

- Records of an analysis conducted to determine which roles, responsibilities and authorities require verification of background.
- Guidance for employees about when/how to perform verification of background.
- 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 verification of background.
- Documentation of follow-up actions taken in response to any issues or discrepancies identified during verification of background.
- Agreements with third-parties that perform verification of background 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

- Review and update, where necessary, procedure for verification of background at least annually.

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.6.1	**BE-CyFun®2023**	BASIC: PR.IP-11.1 IMPORTANT: PR.IP-11.2
NIST VSF v2.0	GV.RR-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	WORKFORCE-1
ETSI EN 319 401	REQ-7.2-10	**EL – Ministerial decision 1027/2019 -**	
CEN/TS 18026:2024	HR-02	**ES-Royal Decree 311/2022**	-

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 EVIDENCES

- Documents such as terms and conditions of employment, contract 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.
- Timely revoke access to network and information systems 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 EVIDENCES

- Records confirming the timely return of entity’s assets.
- Records confirming the timely revocation of access rights.
- Copies of written notifications to the employee about the termination 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.
- Conduct thorough exit interviews to remind departing employees of their ongoing security responsibilities. Use this opportunity to 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. Maintain the history of changes in order to ensure that it remains effective.
- Take into account changes or past incidents when reviewing the process
- Involve legal and HR departments in the review process to ensure comprehensive coverage.

EXAMPLES OF EVIDENCES

- Records of all contractual agreements, NDAs, exit interviews, access revocations, and any legal actions 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 according to a process.
- Documentation of process for personnel changes, including, responsibilities for managing changes, description of rights of access and possession of assets per role, procedures for briefing and training personnel in new roles (e.g. standardized checklists used during the termination process to ensure all necessary steps are taken).

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.6.5	**BE-CyFun®2023**	BASIC: ID.GV-3.1, PR.AC-4.3, PR.IP-11.1 IMPORTANT: PR.IP-11.2
NIST CSF v2.0	GV.RR-04	**FI-Kybermittari**	WORKFORCE-1, ACCESS-1, ACCESS-2, ACCESS-3
ETSI EN 319 401		**EL – Ministerial decision 1027/2019 -**	
CEN/TS 18026:2024	HR-05, HR-06	**ES-Royal Decree 311/2022**	Annex II: 3.2

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 security of 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, GDPR).
- Communicate the process to employees.
- Protect the identity of individuals subject to disciplinary action, where possible, in line with applicable requirements.

EXAMPLES OF EVIDENCES

- Disciplinary process documentation which outlines the types of violations which may be subject to disciplinary actions, and which steps to be taken 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, 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 EVIDENCES

- Review and update records 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 overall disciplinary process of the entity, 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:
  a) the nature (who, what, when, how) and gravity of the violation and its consequences;
  b) whether the offence was intentional (malicious) or unintentional (accidental);
  c) whether or not this is a first or repeated offence;
  d) whether or not the employee that did the violation was properly trained.
- Use the process as 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 to promote and encourage good behaviour.

EXAMPLES OF EVIDENCES

- Disciplinary process documentation which outlines the types of violations which may be subject to disciplinary actions, and which steps to be taken when a violation occurs.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	5.28, A.6.4	**BE-CyFun®2023**	BASIC: ID.GV-3.1 IMPORTANT: ID.GV-3.2
NIST CSF v2.0	ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	WORKFORCE-1
ETSI EN 319 401	REQ-7.2-05	**EL – Ministerial decision 1027/2019 -**	
CEN/TS 18026:2024	HR-01	**ES-Royal Decree 311/2022**	Annex II: 3.2

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.

EXAMPLES OF EVIDENCES

- Access control policy document or documents which outline 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 the access control management, assign specific roles to groups.
    - Access control rules can be implemented in different granularity, 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 in order 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;
    - considering 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;
    - considering 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 EVIDENCES

- Access control policy document which outlines the access control requirements, procedures, and responsibilities.
- User access lists showing the list of users and their corresponding access levels to various network and information systems.

- Authentication protocols, meaning documentation of the authentication methods in place, such as multi-factor authentication.
- Authorization mechanisms with details how permissions are granted, reviewed, and revoked, ensuring that access rights are in line with roles, responsibilities and authorities of users.
- Access logs that record user access activities, which can be used to track and audit user behaviour within the system.
- 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, 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 EVIDENCES

- 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.
- Review and update records showing that the policies are reviewed regularly and updated as necessary.
- Reports from internal or external audits that assess the effectiveness and compliance of the access control policy.

TIPS

GUIDANCE

- Consider the two most frequently overarching principles used in the context of access control:
  - need-to-know: an entity is only granted access to the information which the that entity requires in order to perform its tasks (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 MAC (mandatory access control), DAC (discretionary access control), RBAC (role-based access control) and ABAC (attribute-based access control) depending on the business needs of the organisation.
- Take into account that access control rules can also contain dynamic elements (e.g., a function that evaluates past accesses or specific environment values).

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.15, A.7.2, A.8.3, A.8.21, A9	**BE-CyFun®2023**	BASIC: ID.AM-5.1, ID.GV-1.1, PR.AC-4.1, PR.IP-11.1
			IMPORTANT: ID.AM-6.1, ID.GV-1.2, PR.AC-2.2, PR.AC-4.6, PR.AC-5.4, PR.AC-6.1, PR.AT-3.2, PR.DS-3.3, PR.DS-5.1, PR.IP-11.2, PR.MA-2.1, DE.AE-3.2, DE.CM-3.3, DE.CM-6.1, DE.CM-7.1
			ESSENTIAL: PR.DS-1.1, PR.DS-3.3, DE.CM-2.2
NIST CSF v2.0	PR.AA-05, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-3
ETSI EN 319 401	REQ-7.4-04A, REQ-7.4-06, REQ-7.4-10	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 8**	Cybersecurity Handbook: Part B: 4.1
			Self-assessment tool: -
CEN/TS 18026:2024	OIS-02, ISP-02, IAM-01	**ES-Royal Decree 311/2022**	Article 17, Annex II: 4.2

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 has access only 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.
- Implement a segregation of duties matrix.
- Establish and follow a process for requesting and approving access, preferably automated. The process should:
  - cover granting access rights to assets upon 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 access control policy and is consistent with other information security requirements such as segregation of duties.
  - consider giving temporary access rights for a limited time period and revoking them at the expiration 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 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 access rights of users who have changed roles or jobs.
  - remove or adjust access rights, which can be done by removal, revocation or replacement of keys, authentication information, identification cards or subscriptions.
- 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 sign agreements acknowledging their access responsibilities and obligations.
- 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 at 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.

EXAMPLES OF EVIDENCES

- 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.
- 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.
- 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.
- Physical inspection results 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 validate that all privileges are authorised, on a recurring schedule at a minimum annually, or more frequently.

EXAMPLES OF EVIDENCES

- 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.

- Review and update records showing that the access rights are reviewed regularly and updated as necessary.

TIPS

GUIDANCE

- Centralize access control for all assets through a directory service or SSO provider, where supported.

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.18, A.9	**BE-CyFun®2023**	BASIC: ID.AM-5.1, ID.GV-1.1, PR.AC-1.1, PR.AC-4.3, PR.IP-11.1 IMPORTANT: ID.AM-6.1, ID.GV-1.2, PR.AC-2.2, PR.AC-6.1, PR.AT-3.2, PR.DS-5.1, PR.IP-11.2, PR.MA-2.1, DE.CM-6.1, DE.CM-7.1 ESSENTIAL: PR.DS-1.1
NIST CSF v2.0	PR.AA-05, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-3, WORKFORCE-1, SITUATION-1, SITUATION-2
ETSI EN 319 401	REQ-7.4-05	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 8**	Cybersecurity Handbook: Part B: 4.3, 4.6, 4.7, 4.8, 2.11, 2.14, 9.9 Self-assessment tool: 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.13, 5.14
CEN/TS 18026:2024	OIS-02, IAM-04, IAM-05, PSS-03, HR-05	**ES-Royal Decree 311/2022**	Article 20, Annex II: 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6

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 access control policy referred to in point 11.1 (i.e., only to individuals with the necessary competence to carry out activities that require privileged access and based on the minimum requirement for their functional roles).
- Identify users who need privileged access[57] to a network and information system (e.g., operating systems, database management systems and applications).

[57] "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.

- Maintain an authorization process and a record of all allocated privileged access rights, which is consistent with the process for granting and revoking access rights (Annex to the Regulation, point 11.2.2).

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.
- Establish specific rules to avoid the use of generic administration user IDs (such as “root”) and manage and protect authentication information of such identities.
- Grant temporary privileged access only for the necessary time to implement approved changes or activities (e.g. for maintenance activities), rather than permanently granting privileged access rights.
    - Consider the frequency of the system administration operations: daily tasks (e.g., backups, 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 like checking email or accessing the web. Use separate user identities for these activities.
- Ensure users are aware of their privileged access rights or when they are in privileged access mode, e.g. using specific user identities, user interface settings or specific equipment.

EXAMPLES OF EVIDENCES

- Measures for privileged access control and monitoring for privileged accounts, including the granting and revoking of 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 EVIDENCES

- Review and update records showing that the 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 that verify the management of access rights aligns with the policy and regulatory requirements.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.2, A.8.18, A.9	**BE-CyFun®2023**	BASIC: PR.AC-1.1, PR.AC-4.3 IMPORTANT: PR.AC-4.7, PR.AT-2.1 ESSENTIAL: PR.AC-4.9
NIST CSF v2.0	ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-3
ETSI EN 319 401	REQ-7.4-07	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 8**	Cybersecurity Handbook: Part B: 4.4, 4.5, 4.7 Self-assessment tool: 5.10, 5.11, 5.12, 5.13
CEN/TS 18026:2024	ISP-02, IAM-05, IAM-06	**ES-Royal Decree 311/2022**	-

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.

EXAMPLES OF EVIDENCES

- Regularly maintained logs that track access to system administration systems[58].
- 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, allow access to system administration systems only to authorised personnel with specific roles (e.g., system administrators, IT staff).
- Physically or logically isolate administrative systems from other application servers, e,g, use network segmentation to create separate zones for system administration systems and other systems, e.g. application servers. If applicable, physically inspect server racks to ensure separation.
- Require strong authentication mechanisms such as multi-factor authentication (MFA) for accessing system administration systems.
- Encrypt communication channels (e.g., SSH, HTTPS) to protect data in transit to and from system administration systems.
- Encrypt sensitive configuration files and credentials stored on system administration systems.

EXAMPLES OF EVIDENCES

- 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

- Regularly audit system logs to monitor usage patterns and identify any unauthorised activities.
- Train personnel on the on the proper use of system administration systems

EXAMPLES OF EVIDENCES

- Regularly maintained logs that track access to administration systems.

[58] 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): a) system monitoring, b) configuration management, c) security management, d) user management and e) back-up and recovery.

- 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 on the proper use of system administration systems, e.g. training materials, attendance records, or completion certificates.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.2, A.8.18	**BE-CyFun®2023**	BASIC: PR.AC-4.4
			IMPORTANT: PR.AC-5.4
NIST CSF v2.0		**FI-Kybermittari**	ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-2, ARCHITECTURE-3, ARCHITECTURE-5
ETSI EN 319 401	REQ-7.4-07	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 8**	Cybersecurity Handbook: -
			Self-assessment tool: -
CEN/TS 18026:2024	OIS-02, IAM-06, IAM-09	**ES-Royal Decree 311/2022**	-

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, at a minimum, should contain the person’s name, username, start/stop dates, the department and the level of privileges for each identity.
  - Establish and maintain an inventory of service identities. The inventory, at a minimum, should contain department owner, review date, and purpose.

EXAMPLES OF EVIDENCES

- Documented policy or procedure related to identity management, if available.
- Reports from internal or external audits that verify 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. This also includes also configuration and initial setup of related authentication services; and
  - providing or revoking specific access rights to the identity, based on appropriate authorization or entitlement decisions (see Annex to the Regulation, point 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.

EXAMPLES OF EVIDENCES

- Identity records, e.g. user profiles with unique identifiers (e.g., usernames, employee IDs), 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 Identity and Access Management (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.

EXAMPLES OF EVIDENCES

- 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

- Validate that all active identities are authorised, on a recurring schedule at minimum quarterly, or more frequently.
- Disable or remove, in a timely fashion, identities which they are no longer required, e.g. delete or disable any dormant identities after a predefined period of days of inactivity, where supported.

EXAMPLES OF EVIDENCES

- Review and update records 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 or inactivity.

TIPS

GUIDANCE

- Centralize identity management through a directory or identity service.

EXAMPLES OF EVIDENCES

- Evidence of the systems in place, such as Identity and Access Management (IAM) solutions.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.16	**BE-CyFun®2023**	BASIC: PR.AC-1.1, PR.AC-4.1
			IMPORTANT: PR.AC-1.2, PR.AC-3.3, PR.AC-4.5, PR.AC-4.7, PR.AC-6.1
			ESSENTIAL: PR.AC-4.9, PR.AC-6.2
NIST CSF v2.0	PR.AA-01, PR.AA-05, PR.AC-02	**FI-Kybermittari**	ACCESS-1
ETSI EN 319 401	REQ-7.4-08	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 8**	Cybersecurity Handbook: Part B: 4.2, 4.3, 4.7
			Self-assessment tool: 5.2, 5.6, 5.7, 5.13
CEN/TS 18026:2024	IAM-02, IAM-03, IAM-06	**ES-Royal Decree 311/2022**	Article 20, Annex II: 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6, 5.1.2

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.
  - Two-Factor Authentication (2FA).
  - Multi-Factor Authentication (MFA).
  - Biometric Authentication.
  - Token-Based Authentication, e.g one-time passcode (OTP).
  - Certificate-Based Authentication.
  - Single Sign-On (SSO).
  - OAuth: An open standard for access delegation, commonly used for token-based authentication and authorization.

EXAMPLES OF EVIDENCES

- 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 Identity and Access Management (IAM) solutions.
- Internal or external audit reports verifying the implementation of secure authentication procedures aligned with the access control policy.

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.

GUIDANCE

- Use unique authentication credentials for all entity's assets. Best practice implementation includes, at 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 of 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. over an authenticated and protected channel); 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
  - force users to change their passwords at first login;

  - 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 re-use of previous passwords;
  - prevent the use of commonly -used passwords and compromised usernames, password combinations from hacked systems;
  - not display passwords on the screen when being entered; and
  - store and transmit passwords in protected form.
- Perform password encryption and hashing according to approved cryptographic techniques for passwords.
- Generate an alert when a potential attempted or successful breach of log-on controls is detected.

EXAMPLES OF EVIDENCES

- Logs or reports related to authentication.
- Compliance audits from internal or external audits that verify 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 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 EVIDENCES

- 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 state-of-the-art and effective against emerging threats.
- Stay updated on advancements in authentication technology and integrate new methods as they become available.

EXAMPLES OF EVIDENCES

- Internal or external audit reports detailing the results of periodic audits on 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 for the following:
  - secret authentication information such as passwords are 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 are solely shared with authorized 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 practices 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 have a minimum length;
  - the same credentials are not used across distinct network and information systems; and
  - the obligation to follow these rules are also included in terms and conditions of employment.

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.17	**BE-CyFun®2023**	BASIC: PR.AC-3.2
			IMPORTANT: PR.AC-1.2, PR.AC-1.4, PR.MA-2.2
			ESSENTIAL: PR.AC-6.2
NISTCSF v2.0	PR.AA-05, PR.AA-03, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-2, ARCHITECTURE-3, ARCHITECTURE-5
ETSI EN 319 401	REQ-7.4-08	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 8**	Cybersecurity Handbook: Part B: 5.1, 5.2, 5.3, 5.4, 5.5, 5.8, 5.10
			Self-assessment tool: 6.1, 6.2, 6.6, 6.7, 6.8, 6.10
CEN/TS 18026:2024	IAM-07, IAM-08	**ES-Royal Decree 311/2022**	Article 20, Annex II: 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6

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 methods based on the entity's security needs and user convenience:
  - SMS-based OTP (One-Time Password): Simple but less secure due to risks like SIM swapping.
  - Authenticator Apps: Generate time-based OTPs.
  - Push Notifications: Send an approval request to a user's device.
  - Hardware Tokens: Physical devices generating OTPs.
  - Biometrics: Fingerprints, facial recognition, etc.

EXAMPLES OF EVIDENCES

- Logs showing MFA being used accessing network and information systems.
- Access control policy outlining how different MFA methods are assigned.

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.
- Analyse user roles and the level of access required by each role to determine appropriate MFA methods.
- Consider multi-factor authentication, in particular when accessing systems from a remote location, accessing system administration systems, access to sensitive information, etc.
- Enforce multi-factor authentication on Internet-facing systems, such as email, remote desktop, and Virtual Private Network (VPNs)[59]
- Define when and how MFA is required (e.g., every login, once per session, for high-risk actions).

EXAMPLES OF EVIDENCES

- 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.

[59] Cyber fundamentals, PR.AC-3, Centre for Cyber Security Belgium, accessible at: https://ccb.belgium.be/sites/default/files/cyberfundamentals/CYFUN_IMPORTANT_EN_20230301.pdf

TIPS

GUIDANCE

- Integrate MFA with Single Sign On (SSO) solutions for seamless access.
- 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.
- Combine multi-factor authentication 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 a MFA provider that fits 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., GDPR).

EXAMPLES OF EVIDENCES

- 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 MFA importance and usage
- Regularly generated reports from MFA systems showing log monitoring activities and any detected suspicious activities.
- Configuration files showing the implementation of additional authentication factors based on predefined rules.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.8.5	**BE-CyFun®2023**	BASIC: PR.AC-3.2
			IMPORTANT: PR.AC-1.2, PR.AC-1.4
NIST CSF v2.0	PR.AA-03	**FI-Kybermittari**	ACCESS1
ETSI EN 319 401	Ref. to clause 2 of CA/Browser Forum network security guide	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 8**	Cybersecurity Handbook: Part B: 5.6, 5.7, 5.9, 10.3
			Self-assessment tool: 6.3, 6.4, 6.5, 6.9, 11.3
CEN/TS 18026:2024	OPS-23, IAM-06, IAM-07	**ES-Royal Decree 311/2022**	Article 20, Annex II: 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6

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 EVIDENCES

- 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 integrity and authenticity of information,
  - ensuring availability, 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 by national law, international agreements or international accepted strategies for information sharing information like the Traffic Light Protocol (TLP).
- Align the classification with the access control policy (Annex to the Regulation, point 11.1)
- Classify assets according to the identified classification levels.
- Classify assets other than information in accordance with the classification of the information, they store, process, handle or protect.

EXAMPLES OF EVIDENCES

- Latest, updated list of the assets of the entity 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 EVIDENCES

- 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 the personnel the classification of assets and associated protection requirements.

EXAMPLES OF EVIDENCES

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

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.9, A.5.12, A.5.13	**BE-CyFun®2023**	BASIC: ID.AM-5.1
NIST CSF v2.0	ID.AM-05	**FI-Kybermittari**	CRITICAL-1, CRITICAL-2, ASSET-1, ASSET-2, RESPONSE-4, THIRD-PARTIES-1
ETSI EN 319 401	REQ-7.3.1-02	**EL – Ministerial decision 1027/2019 Article 4 - paragraph 2**	Cybersecurity Handbook: Part B: 1.4
			Self assessment tool: 2.5, 2.6
CEN/TS 18026:2024	AM-05	**ES-Royal Decree 311/2022**	Article 40, Annex II: 4.3.1, 4.1.1

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 and service providers, and any other third party who uses or handles assets of the entity, are aware of the policy.

EXAMPLES OF EVIDENCES

- Policy for the proper handling of assets.
- User manuals or instructions provided to employees, direct suppliers and service providers, and any other third party who uses or handles assets of the entity.
- Documentation showing that employees have completed training sessions on the asset handling policy
- Forms or electronic records where employees, direct suppliers and 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 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.
  - Define protocols for secure transfer.
  - Outline methods for data wiping and physical destruction, ensuring complete and irretrievable deletion.
- Cover the correct usage of any asset used outside the entity’s premises (e.g., mobile device) in the policy.
- 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 EVIDENCES

- Documented policy for handling assets.
- User access lists, access request forms, and approval records.
- Incident reports related to asset handling (e.g., loss, theft, 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, at least annually, the policy for asset handling.

EXAMPLES OF EVIDENCES

- Up-to date policy for asset handling
- Review records or history of changes.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.9, A.5.10, A.5.14, A.7.10	**BE-CyFun®2023**	BASIC: ID.AM-1.1, ID.AM-3.1, ID.GV-4.1 IMPORTANT: ID.AM-1.2, ID.AM-6.1, ID.RA-6.1, PR.DS-3.2, PR.DS-3.3
NIST CSF v2.0	ID.IM-01	**FI-Kybermittari**	PROGRAM-2, ASSET-1, ASSET-2, ASSET-5, ARCHITECTURE-5, ARCHITECTURE-6, WORKFORCE-1
ETSI EN 319 401	REQ-7.3.2	**EL – Ministerial decision 1027/2019 Article 4 - paragraph 2**	Cybersecurity Handbook: Part B: 1.1, 1.3, 1.6, 1.7, 1.8 Self assessment tool: 2.1, 2.2, 2.4, 2.7, 2.8, 2.9, 2.10
CEN/TS 18026:2024	ISP-02, AM-02, AM-03	**ES-Royal Decree 311/2022**	Article 40, Annex II: 4.3.1

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.
- Communicate the policy to employees and third parties who handle removable storage media in order to ensure that they are aware of the policy.

EXAMPLES OF EVIDENCES

- Documented policy on the management of removable media, including at least the points in 12.3.2.
- 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 where 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 (requirement 12.1) and include at least the following:
    - definitions and scope of removable media;
    - authorization requirements;
    - usage guidelines;
    - 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 automatic execution of potentially malicious software.
- In the case where connection of removable media is not prohibited for an organisational (business) reason, removable media should be scanned for malicious code with up-to-date software against malicious code before they are connected to the entity's network and information systems;
- 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 such as secure storage locations and tracking logs for portable storage devices.

EXAMPLES OF EVIDENCES

- 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 EVIDENCES

- Up-to date removable media policy.
- Review records or history of changes.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.7.7, A.7.10	**BE-CyFun®2023**	BASIC: PR.DS-3.1
			IMPORTANT: ID.GV-1.2, PR.PT-1.1, PR.PT-2.2
			ESSENTIAL: PR.DS-1.1, PR.DS-3.4
NIST CSF v2.0	PR.DS-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ARCHITECTURE-3g, ARCHITECTURE-5g, ARCHITECTURE-6c
ETSI EN 319 401	REQ-7.3.2	**EL – Ministerial decision 1027/2019 Article 4 - paragraph 2**	Cybersecurity Handbook: Part B: 1.5
			Self assessment tool: 2.2, 3.11
CEN/TS 18026:2024	ISP-02, AM-02, PS-04	**ES-Royal Decree 311/2022**	Annex II: 5.3.3

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 (see also Annex to this regulation, point 6.4)
- Use standardized naming conventions and categorization methods to maintain consistency across the inventory.
- Make sure that inventory entries contain the data in the guidance above (sampling).
- Implement validation rules within the inventory to ensure data entered is complete and consistent.

EXAMPLES OF EVIDENCES

- Documentation for the inventory of assets
- Up to date inventory of assets
- Review records 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 entities' operations and services.

GUIDANCE

- Consider adding the following to the inventory (indicative, non-exhaustive list):
  - asset unique ID;
  - asset's type, e.g. software including virtual machines (version), hardware (operating system/firmware), services, facilities, HVAC systems, personnel, physical records;
  - asset owner;
  - 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 asset;
  - asset end of life, where applicable; and
  - logging requirements.

EXAMPLES OF EVIDENCES

- 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.
- History of changes is maintained.

EXAMPLES OF EVIDENCES

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

TIPS

GUIDANCE

- Use a tool that supports the comprehensive tracking and management of assets.
- Ideally, the tool supports automated discovery of assets and regular scan for new assets and update of the inventory. 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 EVIDENCES

- Configuration settings of the asset management tool.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.9	**BE-CyFun®2023**	BASIC: ID.AM-1.1, ID.AM-2.1 IMPORTANT: ID.AM-1.2, ID.AM-1.3, ID.AM-2.2, ID.AM-2.4, PR.DS-3.3, DE.CM-7.1
NIST CSF v2.0	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-07, ID.AM-08, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	ASSET-1, ASSET-4
ETSI EN 319 401	REQ-7.3	**EL – Ministerial decision 1027/2019 Article 4 - paragraph 2**	Cybersecurity Handbook: Part B: 1.2, 1.9, 1.10 Self assessment tool: 2.3, 2.11
CEN/TS 18026:2024	AM-04	**ES-Royal Decree 311/2022**	-

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 (point 12.4.1), which can include (indicative, non-exhaustive list):
  - user endpoint devices;
  - portable storage devices;
  - specialised equipment;
  - authentication hardware (e.g., access cards, mechanical keys, physical tokens and smartcards);
  - physical copies of information.

EXAMPLES OF EVIDENCES

- 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 record of the implementation of the policy (list of employees who have left or contractors whose contracts have ended and list of assets they returned, including return date).
- Make sure that relevant terms are part of the employment or service contract.
- Communicate to employees the procedures during the induction process and also 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 authorized 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 EVIDENCES

- Personnel is 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 as well as those they returned.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A.5.11, A.5.18, A.8.24	**BE-CyFun®2023**	BASIC: PR.IP-11.1
			IMPORTANT: PR.AT-3.2, PR.IP-11.2
NIST CSF v2.0		**FI-Kybermittari**	WORKFORCE-1
ETSI EN 319 401	REQ-7.3.2	**EL – Ministerial decision 1027/2019 -**	
CEN/TS 18026:2024	AM-01	**ES-Royal Decree 311/2022**	Annex II: 5.5.5

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 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 (Heating, Ventilation, and Air Conditioning): To maintain optimal operating conditions.
  - Telecommunications: Internet and network connectivity.
- Include in the risk assessment the potential failure and disruption in supporting utilities.

EXAMPLES OF EVIDENCES

- 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.

GUIDANCE

- Consider the availability of supporting utilities in the business continuity plan (Annex to the Regulation, point 4.1).
- Consider the availability of supporting utilities, when implementing backup management (Annex to the Regulation, point 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 (UPS), 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 EVIDENCES

- 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 EVIDENCES

- 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

- Make employees aware of dependencies to supporting utilities.
- Train staff on how to respond effectively to failures and disruptions of supporting utilities.
- Set up monitoring systems to detect utility failures or disruptions.

EXAMPLES OF EVIDENCES

- Records of internal communications, emails, or newsletters highlighting the importance of supporting utilities and their impact on operations.
- Logs demonstrating the detection and recording of any utility failures or disruptions.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A. 7.11	**BE-CyFun®2023**	BASIC: ID.GV-3.1, RS.IM-1.1
			IMPORTANT: ID.BE-1.1, ID.GV-3.2, PR.IP-7.1, PR.IP-9.1, DE.CM-2.1, DE.CM-6.1, DE.CM-6.2, DE.DP-3.1, DE.DP-5.1, RS.IM-1.2, RS.IM-2.1, RC.IM-1.1
			ESSENTIAL: ID.BE-1.2, PR.IP-7.2, PR.IP-7.3, PR.IP-9.2, DE.CM-2.2, DE.DP-5.2
NIST CSF v2.0	DE.CM-02, DE.CM-06, GV.OC-03, GV.OC-05, GV.OC-07, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	RESPONSE-4, CRITICAL-3
ETSI EN 319 401	For network connections REQ-7.8-12	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 9**	Cybersecurity Handbook: Part B: 15.5
			Self-assessment tool: 16.6
CEN/TS 18026:2024	PS-05	**ES-Royal Decree 311/2022**	Annex II: 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7

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.
  - 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.

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.
- Consider the following examples of physical and environmental threats (indicative, non-exhaustive list):
  - fire,
  - flood,
  - earthquake,
  - explosion,
  - theft/vandalism,
  - civil unrest,
  - toxic waste/chemical spill,
  - climate change,
  - pollution/environmental emissions.
- 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, physical barriers)
  - Surveillance systems (e.g. CCTV, entry points, exits, locking mechanisms, security personnel)
  - Climate control (e.g. Temperature and humidity controls, HVAC systems)
  - Fire prevention and response measures (e.g. fire alarms, smoke detectors, sprinkler systems, fire extinguishers)
  - Flood protection measures (e.g. barriers, water sensors, pumps)
- 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 EVIDENCES

- 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 like 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 EVIDENCES

- Detailed reports of the tests conducted, including objectives, procedures, results, and any identified issues.
- 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 assets of high criticality.

EXAMPLES OF EVIDENCES

- Documented physical and environmental security policy, including description of facilities and network and information systems in scope.
- Results of periodic simulations and awareness raising activities.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A. 7.3, A.7.5	**BE-CyFun®2023**	BASIC: RS.IM-1.1
			IMPORTANT: PR.IP-5.1, PR.IP-7.1, PR.IP-9.1, DE.DP-3.1, DE.DP-5.1, RS.IM-1.2, RS.IM-2.1, RC.IM-1.1
			ESSENTIAL: PR.IP-5.2, PR.IP-7.2, PR.IP-7.3, PR.IP-9.2, DE.DP-5.2
NIST CSF v2.0	PR.IR-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	RISK-1, RISK-2, RISK-3, RISK-4, THREAT-2, RESPONSE-3
ETSI EN 319 401	Clause 7.6	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 9**	Cybersecurity Handbook: Part B: 15.5
			Self-assessment tool: 16.6
CEN/TS 18026:2024	PS-05	**ES-Royal Decree 311/2022**	Annex II: 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7

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, which takes into account the measures for protection against physical and environmental threats.

EXAMPLES OF EVIDENCES

- Documented policy for physical security measures, including 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

- Consider in the risk assessment risks associated with unauthorised physical access, damage, and interference to network and information systems.
- Based on the results of the risk assessment determine the assets of high criticality and the impact of their compromise. 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 areas with high criticality.
    - electronic control of entrance and audit trail.
    - segmentation of spaces 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 perimeter.
    - guards and/or alarms to monitor every physical access point to the facility where the information system resides,24 hours per day, 7 days per week.
- Develop and enforce procedures for granting, reviewing, and revoking physical access rights (see Annex to the Regulation, point 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 level.

EXAMPLES OF EVIDENCES

- Risk assessment results

- Existence of physical security measures
- Procedures for granting, reviewing, and revoking physical access rights according to Annex to the Regulation, point 11.2.

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 includes, unannounced attempts to bypass or circumvent measures associated with physical access points to the facility.
- Perform security checks at the physical boundary of the facility or network and information system for unauthorized exfiltration of information or removal of information system components.

EXAMPLES OF EVIDENCES

- Periodic simulations and awareness raising activities to assess the readiness of personnel and the adequacy of the procedures to physical access control.
- Schedule and results of tests and security checks.
- Up to date list of personnel with authorized physical access to facilities.

TIPS

GUIDANCE

- Enforce physical access authorization to network and information systems in addition to the physical access controls for the facility.
- Remove individuals from the facility access list when 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 according to security policies and procedures. Maintain visitor's access records 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 the 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 defined time period, according to GDPR.
- Keep physical access records as dictated by applicable regulations or based on an entity-defined period by approved policy. Keep and store physical access records in case of an audit or investigation.
- Respect risk assessment results before taking actions on damaged devices containing sensitive data.

EXAMPLES OF EVIDENCES

- Perimeter incident response procedures is in place.

- Personnel clearly display the identity.

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	A. 7.1, A.7.2, A.7.4	**BE-CyFun®2023**	BASIC: ID.GV-1.1, PR.AC-2.1, PR.AC-3.1, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.IP-11.1
			IMPORTANT: ID.AM-6.1, ID.GV-1.2, PR.AC-2.2, PR.AC-3.3, PR.AC-4.6, PR.AC-6.1, PR.AT-3.2, PR.DS-3.3, PR.DS-5.1, PR.IP-11.2, PR.MA-2.1, DE.CM-2.1, DE.AE-3.2, DE.CM-6.1, DE.CM-7.1
			ESSENTIAL: PR.AC-2.3, PR.AC-2.4, PR.AC-3.4, PR.AC-4.8, PR.DS-1.1, DE.CM-2.2
NIST CSF v2.0	PR.AA-06, DE.CM-02	**FI-Kybermittari**	RISK-1, RISK-2, RISK-3, ARCHITECTURE-3, ACCESS-3
ETSI EN 319 401	Clause 7.6	**EL – Ministerial decision 1027/2019 - Article 4 - paragraph 9**	Cybersecurity Handbook: Part B: 15.1, 15.2, 15.3, 15.4, 15.6
			Self-assessment tool: 16.1, 16.2, 16.3, 16.4, 16.5, 16.7
CEN/TS 18026:2024	PS-01, PS-02, PS-03, PS-04	**ES-Royal Decree 311/2022**	Annex II: 4.2.5, 4.2.6

ANNEX I NATIONAL FRAMEWORKS

Belgium

Belgium has completed the transposition of the NIS2 directive and transposed it into national legislation. In that legislation, a special role is reserved for the CyberFundamentals framework (CyFun® - www.cyfun.eu).

Finland

Traficom’s (the Finnish Transport and Communications Agency) national recommendation on cybersecurity risk management measures for supervisory authorities and the Cybermeter/Kybermittari 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 enables organisations to do self-assessment on their cybersecurity capabilities and optimize their security investments. Voluntary sharing quantitative self-assessment data to NCSC-FI enables creation of benchmarking data and improves situation awareness of NCSC-FI. The Cybermeter/Kybermittari is a maturity model and developed by the National Cyber Security Centre (NCSC-FI) and it is based on Cybersecurity Capability Maturity Model (C2M2) and the NIST Cybersecurity Framework.

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

Greece

The Greek Cybersecurity Framework consists of:

a) the law 4577/2018 and the ministerial decision 1027/2019;

b) the Cybersecurity Handbook available at: https://mindigital.gr/wp-content/uploads/2022/09/Cybersecurity-Handbook-English-version.pdf; and

c) the self-assessment tool, available at: https://mindigital.gr/wp-content/uploads/2022/11/Cybersecurity-Self-Assessment-Tool-English-version.zip .

The Cybersecurity Handbook and the self-assessment tool are based on globally accepted international standards and guidelines (CIS Controls, ISO 27002, NIST 800-53, OWASP, etc.) and will be dynamically modified to follow changes in standards, the current threat landscape and the legal and regulatory framework.

Spain

The Royal Decree 311/2022, of May 3, regulates the National Security Framework or National Security Framework (ENS or NSF), which is the legal regulation of mandatory compliance for all entities of the Spanish public sector and also of mandatory application to the information systems used by private companies to provide services to the above mentioned public entities.

The full text of the ENS 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

Information. Data in context. In the text, we use primarily information, unless we refer specifically to data (e.g. data breach etc.).

Entity. the relevant entities in scope of the Commission Implementing Regulation (EU) 2024/2690. In other standards or good practices, the terms organisation or enterprise or business may be used.

Asset. Anything that has value to the entity including information. Overall, the assets of a network and information system are personnel, processes, information, software and hardware.

Management bodies as in the context of Article 20 of the NIS2 Directive.

Policy: intentions and direction of an organization, as formally expressed by its management bodies.

Topic-specific policy: a policy on a specific subject or topic, as formally expressed by the relevant to the topic management bodies.

Process: an activity which transforms an input to output.

Procedure: specified way to carry out an activity or a process[60]. The entity can document their needs for more detailed information in a way that is efficient for them beyond the policy. This is mainly procedures and processes.

Rule: accepted principle or instruction that states the entity's expectations on what is required to be done, what is allowed or not allowed. Rules can be formally expressed in topic-specific policies and in other types of documents.[61]

User: all legal and natural persons which have access to the entity's network and information systems (Recital (10) of the Regulation).

Personnel: persons doing work under the entity's direction[62]. 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.

Direct suppliers and service providers, including their personnel.

Measure: this term refers to a cybersecurity risk-management measure as referred to in NIS2. It is used similarly to the term 'control,' which denotes a measure that modifies risk[63]. Additionally, the terms 'measure' and 'protection measure' are used interchangeably.

Facilities: the physical location housing entity's network and information systems.

Event: refers to an information security event meaning an identified occurrence indicating a possible information security breach or failure of controls[64].

Suspicious event: an event that appears unusual or a previously unknown situation which might be a potential security threat. To make clearer the difference between an event and a suspicious event consider an example when a legitimate user fails to login once due to a typo error. This is an event. However, the situation where a user fails to login after five attempts this might be considered a suspicious event.

Incident: an event compromising 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 (NIS2 Article 6 Nr 6).

Significant incident: an incident which meets the criteria of Article 3 of the Regulation.

Crisis: 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[24].

Incident handling. any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident (NIS2 Article 6 Nr 8).

Critical: one of the classification levels assigned to entity's assets following an assessment of their criticality, including the asset classification (point 12.1 of the Annex of the Regulation).

[60] [SOURCE:ISO 30000:2009, 3.12]
[61] [SOURCE: ISO/IEC 27002:2022, 3.1.32]
[62] [SOURCE: ISO/IEC 27002:2022, 3.1.20]
[63] [SOURCE: ISO/IEC 27002:2022, 3.1.8]
[64] [SOURCE: ISO/IEC 27002:2022, 3.1.14]

Privileged access. refers to the necessary permissions granted to specific users of the network and the information system of the entity, in order for them to perform tasks which regular users cannot.

Cyber hygiene practices. Preamble 20 of the Regulation addresses cyber hygiene practices for two target groups under the Directive 2022/2555: (a) essential and important entities, and (b) for their users. Cyber hygiene practices for essential and important entities refer to a common baseline set of practices, which are already covered by the technical and methodological requirements of cybersecurity risk-management measures outlined in the Annex to this Regulation. Therefore, no additional guidance for cyber hygiene practices for essential and important entities is deemed necessary. Cyber hygiene practices referring to users are explicitly mentioned in the guidance and are included in section 8.1 of this guidance.

XX-00-00-000-XX-X

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 000-00-0000-000-0
doi: 0000.0000/000000