ETSI TR 104 168 V1.1.1 (2025-09)

TECHNICAL REPORT

Cyber Security (CYBER);
Critical Security Controls for
Network and Information Security Directive 2 (NIS2)

Reference
DTR/CYBER-00164

Keywords
cyber security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document provides a mapping of the Critical Security Controls [i.10] to support NIS2 Directive provisions.

Introduction

The present document is one of several ETSI publications [i.8], [i.11], [i.12], [i.13] and [i.14] directed at supporting the EU NIS2 Directive and related legislative instruments [i.1], [i.2], [i.3], [i.4], [i.5], [i.6] and [i.7].

1 Scope

The present document item provides a mapping between the Critical Security Controls and NIS2 provisions.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.2] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.3] Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[i.4] Resolution (EC) 13084/1/20: "Council Resolution on Encryption - Security through encryption and security despite encryption".

[i.5] Recommendation 2003/361/EC: "Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises".

[i.6] 2020/0365 (COD), COM(2020) 829 Final: "Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities".

[i.7] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

[i.8] ETSI TR 103 456: "CYBER; Implementation of the Network and Information Security (NIS) Directive".

[i.9] Center for Internet Security: "CIS Controls v8.1, Mapping to NIS2 Directive 2022/2555".

[i.10] ETSI TS 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.11] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.12] ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".

[i.13] ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.14] ETSI TS 103 992: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

COTS	Commercial Off The Shelf
CSC	Critical Security Controls
CSF	Computer Security Framework
DHCP	Dynamic Host Configuration Protocol
ERM	Enterprise Risk Management
IG1	Implementation Group 1
IG2	Implementation Group 2
IG3	Implementation Group 3
NIS2	Network and Information Security Directive 2
SSO	Single Sign-On

4 Applying the Critical Security Controls for effective implementation of the NIS2 Directive

4.1 Methodology and Use

Methodology

The methodology used to create the mapping can be useful to anyone attempting to understand the relationships between the Critical Security Controls and NIS2. The overall goal for Control mappings is to be as specific as possible, leaning towards under-mapping versus over-mapping. The general strategy used is to identify all of the aspects within a control and attempt to discern if both items state the same thing. For instance:

Control 6.1 - Establish an Access Granting Process

Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. For a defensive mitigation to map to this CSC Safeguard it is required by NIS2 to have at least one of the following:

- A clearly documented process, covering both new employees and changes in access.
- All relevant enterprise access control is required by NIS2 to be covered under this process, there can be no separation where different teams control access to different assets.

- Automated tools are ideally used, such as a SSO provider or routing access control through a directory service.
- The same process is followed every time a user's rights change, so a user never amasses greater rights access without documentation.

If the two concepts are effectively equal, they are mapped with the relationship "equivalent". If they are not equal but still related, the exact type of relationship between two defensive mitigations can be further explored. The relationships can be further analysed to understand how similar or different the two defensive mitigations are. The relationship column will contain one of four possible values:

- Equivalent: The defensive mitigation contains the exact same security concept as the Control.
- Superset: The Control is partially or mostly related to the defensive mitigation in question, but the Control is broader in concept.
- Subset: The Safeguard is partially or mostly related yet is still subsumed within the defensive mitigation. The defensive mitigation in question is broader in concept than the Control.
- No relationship: This will be represented by a blank cell.

The relationships should be read from left to right, like a sentence. Control Safeguard X is Equivalent to this < >.

EXAMPLES: Safeguard 16.8 "Separate Production and Non-Production Systems" is EQUIVALENT to NIST CSF PR.DS-7 "The development and testing environment(s) are separate from the production environment".

Safeguard 3.5 "Securely Dispose of Data" is a SUBSET of NIST CSF PR.DS-3 "Assets are formally managed throughout removal, transfers, and disposition".

The Critical Security Controls are written with certain principles in mind, such as only having one ask per Safeguard. This means many of the mapping targets are written in a way that contain multiple Safeguards within the same defensive mitigation, so the relationship can often be "Subset".

Mappings are available from a variety of sources online, and different individuals may make their own decisions on the type of relationship. Critical Security Controls mappings are intended to be as objective as possible, and improvements are encouraged.

Use

The clauses in the Critical Security Controls concerning delineation of Asset Types, Security Functions, and Implementation Groups apply to the mappings below. For reference, these delineations are repeated in part here.

Asset Types are shown in Figure 4.1-1.

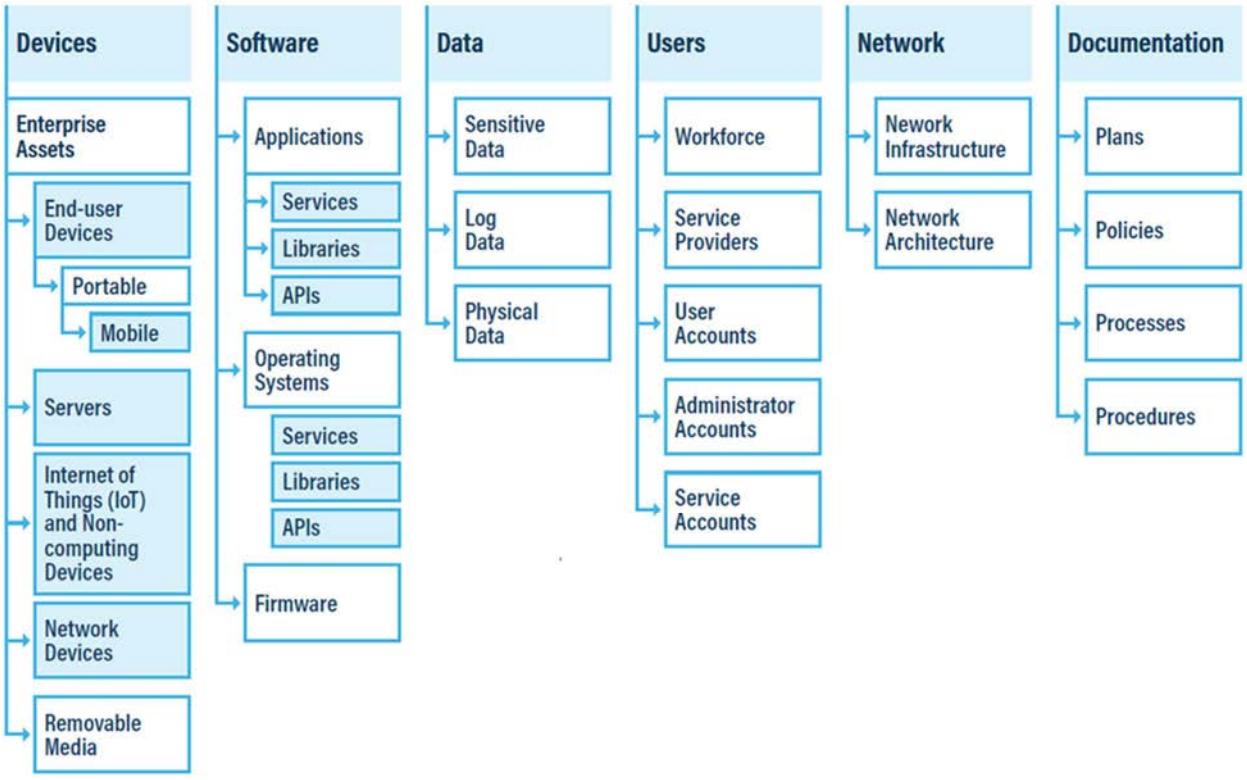

Figure 4.1-1

Security Functions include:

- GOVERN - The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader Enterprise Risk Management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

- IDENTIFY - The organization's current cybersecurity risks are understood. Understanding the organization's assets (e.g. data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.

- PROTECT - Safeguards to manage the organization's cybersecurity risks are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e. securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.

- DETECT - Possible cybersecurity attacks and compromises are found and analysed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.

- RESPOND - Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.

- RECOVER - Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

Implementation Groups include:

- **IG1.** An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.

- Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office Commercial Off-The-Shelf (COTS) hardware and software.

- **IG2 (Includes IG1).** An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units can have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.

- Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

- **IG3 (Includes IG1 and IG2).** An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g. risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise should address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

  Safeguards selected for IG3 should abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

4.2 Applicability Overview

Table 4.2-1: Applicability of the Critical Security Controls to the NIS2 Directive

Control	Safeguard Title	Applicability
1	Inventory and Control of Enterprise Assets	1 of 5
2	Inventory and Control of Software Assets	1 of 7
3	Data Protection	9 of 14
4	Secure Configuration of Enterprise Assets and Software	4 of 12
5	Account Management	4 of 6
6	Access Control Management	8 of 8
7	Continuous Vulnerability Management	7 of 9
8	Audit Log Management	10 of 12
9	Email and Web Browser Protections	2 of 7
10	Malware Defences	3 of 7
11	Data Recovery	4 of 5
12	Network Infrastructure Management	5 of 8
13	Network Monitoring and Defence	2 of 11
14	Security Awareness and Skills Training	3 of 9
15	Service Provider Management	6 of 7
16	Application Software Security	2 of 14
17	Incident Response Management	8 of 9
18	Penetration Testing	1 of 5

4.3 Applying the Critical Security Controls and Safeguards

Table 4.3-1 below provides a mapping by the Critical Security Controls community to the NIS2 provisions to support the indicated requirements [i.9].

Table 4.3-1

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
1			**Inventory and Control of Enterprise Assets**								
1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	x	x	x	Superset	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.
1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	x	x	x	Superset	12.4	Asset inventory	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.
1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	x	x	x	Superset	12.4	Asset inventory	12.4.3	The relevant entities shall regularly review and update the inventory and their assets and document the history of changes.
1.2	Devices	Respond	Address Unauthorized Assets	x	x	x					
1.3	Devices	Detect	Utilize an Active Discovery Tool		x	x					
1.4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		x	x					
1.5	Devices	Detect	Use a Passive Asset Discovery Tool			x					
2			**Inventory and Control of Software Assets**								
2.1	Software	Identify	Establish and Maintain a Software Inventory	x	x	x					

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
2.2	Software	Identify	Ensure Authorized Software is Currently Supported	x	x	x	Subset	6.6	Security patch management	6.6.2	By way of derogation from point 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.
2.3	Software	Respond	Address Unauthorized Software	x	x	x					
2.4	Software	Detect	Utilize Automated Software Inventory Tools		x	x					
2.5	Software	Protect	Allowlist Authorized Software		x	x					
2.6	Software	Protect	Allowlist Authorized Libraries		x	x					
2.7	Software	Protect	Allowlist Authorized Scripts			x					
3			**Data Protection**								
3.1	Data	Govern	Establish and Maintain a Data Management Process	x	x	x	Superset	9.1	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 information in line with the relevant entities' information classification and the results of the risk assessment.
3.1	Data	Govern	Establish and Maintain a Data Management Process	x	x	x	Subset	12.2	Handling of information and assets	12.2.1	The relevant entities shall establish, implement and apply a policy for the proper handling of information and assets in accordance with their network and information security policy, and shall communicate the policy to anyone who uses or handles information and assets.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
3.1	Data	Govern	Establish and Maintain a Data Management Process	x	x	x	Subset	12.2	Handling of information and assets	12.2.2	The policy shall: (a) cover the entire life cycle of the information and 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 information and assets; (c) provide that equipment, hardware, software and data may be transferred to external premises only after approval by bodies authorized by management bodies in accordance with the policies, (d) provide that the transfer shall take place in a secure manner, in accordance with the type of asset or information to be transferred.
3.1	Data	Govern	Establish and Maintain a Data Management Process	x	x	x	Subset	12.2	Handling of information and assets	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.
3.2	Data	Identify	Establish and Maintain a Data Inventory	x	x	x					
3.3	Data	Protect	Configure Data Access Control Lists	x	x	x	Subset	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 of persons and processes on network and information systems, based on business requirements as well as network and information system security requirements.
3.4	Data	Protect	Enforce Data Retention	x	x	x					

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
3.5	Data	Protect	Securely Dispose of Data	x	x	x	Subset	12.2	Handling of information and assets	12.2.2	The policy shall: (a) cover the entire life cycle of the information and 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 information and assets; (c) provide that equipment, hardware, software and data may be transferred to external premises only after approval by bodies authorized by management bodies in accordance with the policies, (d) provide that the transfer shall take place in a secure manner, in accordance with the type of asset or information to be transferred.
3.6	Data	Protect	Encrypt Data on End-User Devices	x	x	x	Subset	9.1	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 information in line with the relevant entities' information classification and the results of the risk assessment.
3.7	Data	Identify	Establish and Maintain a Data Classification Scheme		x	x	Subset	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 information and assets in scope of their network and information systems for the level of protection required.
3.7	Data	Identify	Establish and Maintain a Data Classification Scheme		x	x	Subset	12.1	Asset classification	12.1.2	For the purpose of point 12.1.1, the relevant entities shall: (a) lay down a system of classification levels for information and assets; (b) associate all information and 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 information and assets with the delivery and recovery objectives set out in their business and disaster recovery plans.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
3.7	Data	Identify	Establish and Maintain a Data Classification Scheme		x	x	Subset	12.1	Asset classification	12.1.3	The relevant entities shall conduct periodic reviews of the classification levels of information and assets and update them, where appropriate.
3.8	Data	Identify	Document Data Flows		x	x					
3.9	Data	Protect	Encrypt Data on Removable Media		x	x	Subset	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.
3.9	Data	Protect	Encrypt Data on Removable Media		x	x	Subset	12.3	Removable media policy	12.3.2	The policy shall: (a) provide for a technical prohibition of the connection of removable media unless there is an organizational 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 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 information on removable storage media.
3.10	Data	Protect	Encrypt Sensitive Data in Transit		x	x					
3.11	Data	Protect	Encrypt Sensitive Data at Rest		x	x					
3.12	Data	Protect	Segment Data Processing and Storage Based on Sensitivity		x	x	Subset	11.4	Administration systems	11.4.1	The relevant entities shall restrict and control the use of system administration systems.
3.12	Data	Protect	Segment Data Processing and Storage Based on Sensitivity		x	x	Subset	11.4	Administration systems	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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
3.13	Data	Protect	Deploy a Data Loss Prevention Solution			x					
3.14	Data	Detect	Log Sensitive Data Access			x	Subset	3.2	Monitoring and logging	3.2.3	The relevant entities shall maintain, document, and review logs. Logs shall include: (a) 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, where appropriate; (j) access to and use of their network equipment and devices; (k) activation, stopping and pausing of the various logs; (l) environmental events, such as flooding alarms, where appropriate.
4			**Secure Configuration of Enterprise Assets and Software**								
4.1	Documentation	Govern	Establish and Maintain a Secure Configuration Process	x	x	x	Subset	6.3	Configuration management	6.3.1	The relevant entities shall establish, document, implement, and monitor configurations, including security configurations of hardware, software, services and networks.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
4.1	Documentation	Govern	Establish and Maintain a Secure Configuration Process	x	x	x	Subset	6.3	Configuration management	6.3.2	For the purpose of point 6.3.1, the relevant entities shall: (a) lay down configurations, including security configurations, for their hardware, software, services and networks; (b) lay down and implement processes and tools to enforce the laid down configurations, including security configurations, for hardware, software, services and networks, for newly installed systems as well as for operational systems over their lifetime.
4.1	Documentation	Govern	Establish and Maintain a Secure Configuration Process	x	x	x	Subset	6.3	Configuration management	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
4.2	Documentation	Govern	Establish and Maintain a Secure Configuration Process for Network Infrastructure	x	x	x	Subset	6.3	Configuration management	6.3.1	The relevant entities shall establish, document, implement, and monitor configurations, including security configurations of hardware, software, services and networks.
4.2	Documentation	Govern	Establish and Maintain a Secure Configuration Process for Network Infrastructure	x	x	x	Subset	6.3	Configuration management	6.3.2	For the purpose of point 6.3.1, the relevant entities shall: (a) lay down configurations, including security configurations, for their hardware, software, services and networks; (b) lay down and implement processes and tools to enforce the laid down configurations, including security configurations, for hardware, software, services and networks, for newly installed systems as well as for operational systems over their lifetime.
4.2	Documentation	Govern	Establish and Maintain a Secure Configuration Process for Network Infrastructure	x	x	x	Subset	6.3	Configuration management	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

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
4.3	Devices	Protect	Configure Automatic Session Locking on Enterprise Assets	x	x	x	Subset	11.6	Authentication	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, and when suspicion that the credential is revealed to an unauthorized person; (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.
4.4	Devices	Protect	Implement and Manage a Firewall on Servers	x	x	x					
4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	x	x	x					
4.6	Devices	Protect	Securely Manage Enterprise Assets and Software	x	x	x					
4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	x	x	x					
4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		x	x					
4.9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets		x	x					

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
4.10	Devices	Protect	Enforce Automatic Device Lockout on Portable End-User Devices		x	x	Subset	11.6	Authentication	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, and when suspicion that the credential is revealed to an unauthorized person; (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.
4.11	Data	Protect	Enforce Remote Wipe Capability on Portable End-User Devices		x	x					
4.12	Data	Protect	Separate Enterprise Workspaces on Mobile End-User Devices			x					
5			**Account Management**								
5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	x	x	x	Subset	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.
5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	x	x	x	Subset	11.6	Authentication	11.6.4	The relevant entities shall regularly review the identities and, if no longer needed, deactivate them without delay.
5.2	Users	Protect	Use Unique Passwords	x	x	x					
5.3	Users	Protect	Disable Dormant Accounts	x	x	x					

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	x	x	x	Subset	11.3	Privileged accounts and system administration accounts	11.3.2	The policies referred to in point 11.3.1 shall: (a) establish strong identification, authentication such as multi-factor authentication, and authorization 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) individualize 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.
5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	x	x	x	Subset	11.6	Authentication	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, and when suspicion that the credential is revealed to an unauthorized person; (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.
5.5	Users	Identify	Establish and Maintain an Inventory of Service Accounts		x	x					
5.6	Users	Protect	Centralize Account Management		x	x					
6			**Access Control Management**								

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
6.1	Documentation	Govern	Establish an Access Granting Process	x	x	x	Subset	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.
6.1	Documentation	Govern	Establish an Access Granting Process	x	x	x	Subset	11.2	Management of access rights	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 authorized by their owner; (d) ensure that access rights appropriately address third-party access, such as suppliers and service providers, in particular by limiting access rights in scope and in duration; EN 21 EN (e) maintain a register of access rights granted; (f) apply logging to the management of access rights.
6.2	Documentation	Govern	Establish an Access Revoking Process	x	x	x	Subset	10.3	Termination or change of employment procedures	10.3.2	For the purpose of point 10.3.1, the relevant entities shall: (a) 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; (b) put in place access control policies which ensure that access rights are modified accordingly upon the individual's termination or change of employment; (c) ensure that, after a change of employment, the employee can perform the new tasks.
6.2	Documentation	Govern	Establish an Access Revoking Process	x	x	x	Subset	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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
6.2	Documentation	Govern	Establish an Access Revoking Process	x	x	x	Subset	11.2	Management of access rights	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 authorized by their owner; (d) ensure that access rights appropriately address third-party access, such as 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.
6.3	Users	Protect	Require MFA for Externally-Exposed Applications	x	x	x	Subset	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.
6.3	Users	Protect	Require MFA for Externally-Exposed Applications	x	x	x	Subset	11.7	Multi-factor authentication	11.7.2	The relevant entities shall ensure that the strength of authentication is appropriate for the classification of the asset to be accessed.
6.4	Users	Protect	Require MFA for Remote Network Access	x	x	x	Subset	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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
6.5	Users	Protect	Require MFA for Administrative Access	x	x	x	Subset	11.3	Privileged accounts and system administration accounts	11.3.2	The policies referred to in point 11.3.1 shall: (a) establish strong identification, authentication such as multi-factor authentication, and authorization 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) individualize 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.
6.5	Users	Protect	Require MFA for Administrative Access	x	x	x	Subset	11.7	Multi-factor authentication	11.7.2	The relevant entities shall ensure that the strength of authentication is appropriate for the classification of the asset to be accessed.
6.6	Software	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems		x	x	Subset	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.
6.7	Users	Protect	Centralize Access Control		x	x	Subset	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.
6.7	Users	Protect	Centralize Access Control		x	x	Subset	11.6	Authentication	11.6.3	The relevant entities shall 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.
6.8	Users	Govern	Define and Maintain Role-Based Access Control			x	Superset	1.2	Roles, responsibilities and authorities	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.
6.8	Users	Govern	Define and Maintain Role-Based Access Control			x	Subset	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 of persons and processes on network and information systems, based on business requirements as well as network and information system security requirements.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
6.8	Users	Govern	Define and Maintain Role-Based Access Control			x	Subset	11.2	Management of access rights	11.2.3	The relevant entities shall review access rights at planned intervals and shall modify them based on organizational changes. The relevant entities shall document the results of the review including the necessary changes of access rights.
6.8	Users	Govern	Define and Maintain Role-Based Access Control			x	Subset	11.3	Privileged accounts and system administration accounts	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 organizational changes, and shall document the results of the review, including the necessary changes of access rights.
7			**Continuous Vulnerability Management**								
7.1	Documentation	Govern	Establish and Maintain a Vulnerability Management Process	x	x	x	Subset	6.6	Security patch management	6.6.1	The relevant entities shall specify and apply 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.
7.1	Documentation	Govern	Establish and Maintain a Vulnerability Management Process	x	x	x	Subset	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.
7.1	Documentation	Govern	Establish and Maintain a Vulnerability Management Process	x	x	x	Subset	6.10	Vulnerability handling and disclosure	6.10.4	The relevant entities shall review and, where appropriate, update at planned intervals the channels they use for monitoring vulnerability information.
7.2	Documentation	Govern	Establish and Maintain a Remediation Process	x	x	x	Subset	6.10	Vulnerability handling and disclosure	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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
7.3	Software	Protect	Perform Automated Operating System Patch Management	x	x	x					
7.4	Software	Protect	Perform Automated Application Patch Management	x	x	x					
7.5	Software	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets		x	x	Subset	6.10	Vulnerability handling and disclosure	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 and incident management procedures; (e) lay down a procedure for disclosing vulnerabilities in accordance with the applicable national coordinated vulnerability disclosure policy.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
7.6	Software	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		x	x	Subset	6.10	Vulnerability handling and disclosure	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 and incident management procedures; (e) lay down a procedure for disclosing vulnerabilities in accordance with the applicable national coordinated vulnerability disclosure policy.
7.7	Software	Respond	Remediate Detected Vulnerabilities		x	x	Superset	6.10	Vulnerability handling and disclosure	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.
8			**Audit Log Management**								
8.1	Documentation	Govern	Establish and Maintain an Audit Log Management Process	x	x	x	Equivalent	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.
8.1	Documentation	Govern	Establish and Maintain an Audit Log Management Process	x	x	x	Superset	3.2	Monitoring and logging	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 minimizes false positives and false negatives.
8.1	Documentation	Govern	Establish and Maintain an Audit Log Management Process	x	x	x	Superset	3.2	Monitoring and logging	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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
8.2	Data	Detect	Collect Audit Logs	x	x	x	Subset	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.
8.3	Data	Protect	Ensure Adequate Audit Log Storage	x	x	x					
8.4	Network	Protect	Standardize Time Synchronization		x	x	Equivalent	3.2	Monitoring and logging	3.2.6	The relevant entities shall ensure that all systems have synchronized 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 independently.
8.5	Data	Detect	Collect Detailed Audit Logs		x	x	Subset	3.2	Monitoring and logging	3.2.3	The relevant entities shall maintain, document, and review logs. Logs shall include: (a) 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, where appropriate; (j) access to and use of their network equipment and devices; (k) activation, stopping and pausing of the various logs; (l) environmental events, such as flooding alarms, where appropriate.
8.6	Data	Detect	Collect DNS Query Audit Logs		x	x					

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
8.7	Data	Detect	Collect URL Request Audit Logs		x	x					
8.8	Data	Detect	Collect Command-Line Audit Logs		x	x					
8.9	Data	Detect	Centralize Audit Logs		x	x	Subset	3.2	Monitoring and logging	3.2.5	The relevant entities shall maintain and back up logs for a predefined period and shall store the logs at a central location and protect them from unauthorized access or changes.
8.10	Data	Protect	Retain Audit Logs		x	x	Subset	3.2	Monitoring and logging	3.2.5	The relevant entities shall maintain and back up logs for a predefined period and shall store the logs at a central location and protect them from unauthorized access or changes.
8.11	Data	Detect	Conduct Audit Log Reviews		x	x	Subset	3.2	Monitoring and logging	3.2.3	The relevant entities shall maintain, document, and review logs. Logs shall include: (a) 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, where appropriate; (j) access to and use of their network equipment and devices; (k) activation, stopping and pausing of the various logs; (l) environmental events, such as flooding alarms, where appropriate.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
8.11	Data	Detect	Conduct Audit Log Reviews		x	x	Subset	3.2	Monitoring and logging	3.2.4	The logs shall be reviewed for any unusual or unwanted trends. 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 responsible employee shall ensure that, in case of an alarm, a qualified and appropriate response is initiated.
8.12	Data	Detect	Collect Service Provider Logs			x					
9			**Email and Web Browser Protections**								
9.1	Software	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	x	x	x					
9.2	Devices	Protect	Use DNS Filtering Services	x	x	x	Subset	6.7	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 unauthorized access; (c) configure controls to prevent accesses 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 authorized by those entities; (h) allow connections of service providers only after an authorization request and for a set time period, such as the duration of a maintenance operation;

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
											(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 secure and full transition towards latest generation network layer communication protocols to reduce the attack surface of the networks 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 Internet routing security and routing hygiene of traffic originating from and destined to the network.
9.3	Network	Protect	Maintain and Enforce Network-Based URL Filters		x	x					
9.4	Software	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		x	x					
9.5	Network	Protect	Implement DMARC		x	x	Subset	6.7	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 unauthorized access; (c) configure controls to prevent accesses 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;

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
											(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 authorized by those entities; (h) allow connections of service providers only after an authorization 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 secure and full transition towards latest generation network layer communication protocols to reduce the attack surface of the networks 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 Internet routing security and routing hygiene of traffic originating from and destined to the network.
9.6	Network	**Protect**	Block Unnecessary File Types		x	x					
9.7	Network	**Protect**	Deploy and Maintain Email Server Anti-Malware Protections			x					

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
10			**Malware Defences**								
10.1	Devices	**Detect**	Deploy and Maintain Anti-Malware Software	x	x	x	Subset	6.9	Protection against malicious and unauthorized software	6.9.1	The relevant entities shall protect their network and information systems against malicious and unauthorized software.
10.1	Devices	**Detect**	Deploy and Maintain Anti-Malware Software	x	x	x	Subset	6.9	Protection against malicious and unauthorized software	6.9.2	For that purpose, the relevant entities shall in particular ensure that their network and information systems are equipped with malware detection and repair software, which is updated regularly in accordance with the with the risk assessment and the contractual agreements with the providers.
10.2	Devices	**Protect**	Configure Automatic Anti-Malware Signature Updates	x	x	x					
10.3	Devices	**Protect**	Disable Autorun and Autoplay for Removable Media	x	x	x	Subset	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.
10.3	Devices	**Protect**	Disable Autorun and Autoplay for Removable Media	x	x	x	Subset	12.3	Removable media policy	12.3.2	The policy shall: (a) provide for a technical prohibition of the connection of removable media unless there is an organizational 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 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 information on removable storage media.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media		x	x	Subset	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.
10.5	Devices	Protect	Enable Anti-Exploitation Features		x	x					
10.6	Devices	Protect	Centrally Manage Anti-Malware Software		x	x					
10.7	Devices	Detect	Use Behaviour-Based Anti-Malware Software		x	x					
11			**Data Recovery**								
11.1	Documentation	Govern	Establish and Maintain a Data Recovery Process	x	x	x	Superset	4.2	Backup management	4.2.1	The relevant entities shall maintain backup copies of information and provide sufficient available resources, including facilities, network and information systems and staff.
11.1	Documentation	Govern	Establish and Maintain a Data Recovery Process	x	x	x	Superset	4.2	Backup management	4.2.2	Based on the results of the risk assessment 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 information 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; EN 8 EN (d) appropriate physical and logical access controls to backup copies, in accordance with the information classification level; (e) restoring information from backup copies, including approval processes; (f) retention periods based on business and regulatory requirements.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
11.1	Documentation	Govern	Establish and Maintain a Data Recovery Process	x	x	x	Superset	4.2	Backup management	4.2.4	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.
11.2	Data	Recover	Perform Automated Backups	x	x	x					
11.3	Data	Protect	Protect Recovery Data	x	x	x	Subset	4.2	Backup management	4.2.2	Based on the results of the risk assessment 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 information 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; EN 8 EN (d) appropriate physical and logical access controls to backup copies, in accordance with the information classification level; (e) restoring information from backup copies, including approval processes; (f) retention periods based on business and regulatory requirements.
11.3	Data	Protect	Protect Recovery Data	x	x	x	Superset	4.2	Backup management	4.2.3	The relevant entities shall perform regular integrity checks on the backup copies.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
11.4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data	x	x	x	Subset	4.2	Backup management	4.2.2	Based on the results of the risk assessment 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 information 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; EN 8 EN (d) appropriate physical and logical access controls to backup copies, in accordance with the information classification level; (e) restoring information from backup copies, including approval processes; (f) retention periods based on business and regulatory requirements.
11.5	Data	Recover	Test Data Recovery		x	x	Equivalent	4.2	Backup management	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.
12			**Network Infrastructure Management**								
12.1	Network	Protect	Ensure Network Infrastructure is Up-to-Date	x	x	x	Subset	6.6	Security patch management	6.6.1	The relevant entities shall specify and apply 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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
12.2	Network	**Protect**	Establish and Maintain a Secure Network Architecture		x	x	Subset	6.7	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 unauthorized access; (c) configure controls to prevent accesses 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 authorized by those entities; (h) allow connections of service providers only after an authorization 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 secure and full transition towards latest generation network layer communication protocols to reduce the attack surface of the networks 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;

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
											(l) apply best practices for Internet routing security and routing hygiene of traffic originating from and destined to the network.
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		x	x	Superset	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.
12.2	Network	Protect	Establish and Maintain a Secure Network Architecture		x	x	Superset	6.8	Network segmentation	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) apply the same security measures to all network and information systems in the same zone; (c) grant access to a network or zone based on an assessment of its security requirements; (d) keep all systems that are critical to the relevant entities operation or to safety in one or more secured zones; (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 entities' services from systems used in development and testing, including backups.
12.3	Network	Protect	Securely Manage Network Infrastructure		x	x					
12.4	Documentation	Govern	Establish and Maintain Architecture Diagram(s)		x	x	Subset	6.7	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 unauthorized access;

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
											(c) configure controls to prevent accesses 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 authorized by those entities; (h) allow connections of service providers only after an authorization 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 secure and full transition towards latest generation network layer communication protocols to reduce the attack surface of the networks 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 Internet routing security and routing hygiene of traffic originating from and destined to the network.
12.4	Documentation	Govern	Establish and Maintain Architecture Diagram(s)		x	x	Subset	6.7	Network security	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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
12.5	Network	**Protect**	Centralize Network Authentication, Authorization, and Auditing (AAA)		x	x					
12.6	Network	**Protect**	Use of Secure Network Management and Communication Protocols		x	x	Subset	6.7	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 unauthorized access; (c) configure controls to prevent accesses 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; EN 14 EN (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 authorized by those entities; (h) allow connections of service providers only after an authorization 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 secure and full transition towards latest generation network layer communication protocols to reduce the attack surface of the networks and establish measures to accelerate such transition;

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
											(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 Internet routing security and routing hygiene of traffic originating from and destined to the network.
12.7	Devices	**Protect**	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		x	x					
12.8	Devices	**Protect**	Establish and Maintain Dedicated Computing Resources for All Administrative Work			x	Subset	6.8	Network segmentation	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) apply the same security measures to all network and information systems in the same zone; (c) grant access to a network or zone based on an assessment of its security requirements; (d) keep all systems that are critical to the relevant entities operation or to safety in one or more secured zones; (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; EN 15 EN (h) separate the production systems for the entities' services from systems used in development and testing, including backups.
13			**Network Monitoring and Defence**								
13.1	Network	**Detect**	Centralize Security Event Alerting		x	x					

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
13.2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution		x	x					
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution		x	x	Subset	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.
13.4	Network	Protect	Perform Traffic Filtering Between Network Segments		x	x					
13.5	Devices	Protect	Manage Access Control for Remote Assets		x	x					
13.6	Network	Detect	Collect Network Traffic Flow Logs		x	x					
13.7	Devices	Protect	Deploy a Host-Based Intrusion Prevention Solution			x					
13.8	Network	Protect	Deploy a Network Intrusion Prevention Solution			x					
13.9	Network	Protect	Deploy Port-Level Access Control			x					
13.10	Network	Protect	Perform Application Layer Filtering			x					
13.11	Network	Detect	Tune Security Event Alerting Thresholds			x	Subset	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.
14			**Security Awareness and Skills Training**								
14.1	Documentation	Govern	Establish and Maintain a Security Awareness Program	x	x	x	Superset	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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
14.1	Documentation	Govern	Establish and Maintain a Security Awareness Program	x	x	x	Subset	8.1	Awareness raising and basic cyber hygiene practices	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.
14.1	Documentation	Govern	Establish and Maintain a Security Awareness Program	x	x	x	Subset	8.1	Awareness raising and basic cyber hygiene practices	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.
14.1	Documentation	Govern	Establish and Maintain a Security Awareness Program	x	x	x	Superset	8.2	Security training	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.
14.2	Users	Protect	Train Workforce Members to Recognize Social Engineering Attacks	x	x	x					
14.3	Users	Protect	Train Workforce Members on Authentication Best Practices	x	x	x					
14.4	Users	Protect	Train Workforce on Data Handling Best Practices	x	x	x					
14.5	Users	Protect	Train Workforce Members on Causes of Unintentional Data Exposure	x	x	x					
14.6	Users	Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	x	x	x	Subset	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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
14.6	Users	Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	x	x	x	Subset	3.3	Event reporting	3.3.2	The relevant entities shall communicate the event reporting mechanism to their suppliers and customers and shall regularly train their employees how to use the mechanism.
14.7	Users	Protect	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	x	x	x					
14.8	Users	Protect	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	x	x	x					
14.9	Users	Protect	Conduct Role-Specific Security Awareness and Skills Training		x	x	Superset	8.2	Security training	8.2.1	The relevant entities shall ensure that employees, whose roles require security relevant skill sets and expertise, receive training on network and information system security.
14.9	Users	Protect	Conduct Role-Specific Security Awareness and Skills Training		x	x	Superset	8.2	Security 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.
14.9	Users	Protect	Conduct Role-Specific Security Awareness and Skills Training		x	x	Superset	8.2	Security 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) regular and documented instructions regarding the secure configuration and operation of the network and information systems, including mobile devices; (b) regular and documented briefing on known cyber threats; (c) regular and documented training of the behaviour when security-relevant events occur.
14.9	Users	Protect	Conduct Role-Specific Security Awareness and Skills Training		x	x	Superset	8.2	Security training	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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
15			**Service Provider Management**								
15.1	Users	**Identify**	Establish and Maintain an Inventory of Service Providers	x	x	x	Subset	5.2	Directory of suppliers and service providers	5.2.1	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 entities.
15.2	Documentation	**Govern**	Establish and Maintain a Service Provider Management Policy		x	x	Subset	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.
15.2	Documentation	**Govern**	Establish and Maintain a Service Provider Management Policy		x	x	Subset	5.1	Supply chain security policy	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 product from suppliers and service providers occur.
15.2	Documentation	**Govern**	Establish and Maintain a Service Provider Management Policy		x	x	Subset	6.1	Security in acquisition of ICT services or ICT products	6.1.1	For the purpose of Article 21(2), point (e) of Directive (EU) 2022/2555, the relevant entities shall set and implement processes and procedures 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, from suppliers or service providers throughout their life cycle.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
15.2	Documentation	Govern	Establish and Maintain a Service Provider Management Policy		x	x	Subset	6.1	Security in acquisition of ICT services or ICT products	6.1.2	For the purpose of point 6.1.1, the processes and procedures 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) appropriate 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.
15.2	Documentation	Govern	Establish and Maintain a Service Provider Management Policy		x	x	Superset	6.1	Security in acquisition of ICT services or ICT products	6.1.3	The relevant entities shall review and, where appropriate, update the processes and procedures at planned intervals and when significant incidents occur.
15.3	Users	Govern	Classify Service Providers		x	x					
15.4	Documentation	Govern	Ensure Service Provider Contracts Include Security Requirements		x	x	Subset	1.2	Roles, responsibilities and authorities	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.
15.4	Documentation	Govern	Ensure Service Provider Contracts Include Security Requirements		x	x	Subset	3.3	Event reporting	3.3.2	The relevant entities shall communicate the event reporting mechanism to their suppliers and customers and shall regularly train their employees how to use the mechanism.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
15.4	Documentation	Govern	Ensure Service Provider Contracts Include Security Requirements		x	x	Subset	5.1	Supply chain security 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, specify 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 skills and training, and where appropriate certifications, required from the suppliers' or service providers' employees; (c) requirements regarding background checks of the suppliers' and service providers' employees pursuant to point 10.2; (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) provisions on repair times; (f) the right to audit or right to receive audit reports; EN 10 EN (g) 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; (h) 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); (i) 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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
15.5	Users	Govern	Assess Service Providers			x	Subset	5.1	Supply chain security policy	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) the ability of the suppliers and service providers to meet cybersecurity specifications set by the 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.
15.5	Users	Govern	Assess Service Providers			x	Subset	5.1	Supply chain security policy	5.1.5	The relevant entities shall take into account the elements referred to in points 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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
15.6	Data	Govern	Monitor Service Providers			x	Subset	5.1	Supply chain security 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, specify 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 skills and training, and where appropriate certifications, required from the suppliers' or service providers' employees; (c) requirements regarding background checks of the suppliers' and service providers' employees pursuant to point 10.2; (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) provisions on repair times; (f) the right to audit or right to receive audit reports; EN 10 EN (g) 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; (h) 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); (i) 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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
15.6	Data	Govern	Monitor Service Providers			x	Subset	5.1	Supply chain security policy	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 product from suppliers and service providers occur.
15.6	Data	Govern	Monitor Service Providers			x	Subset	5.1	Supply chain security policy	5.1.7	For the purpose of point 5.1.5, 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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
15.7	Data	**Protect**	Securely Decommission Service Providers			x	Subset	5.1	Supply chain security 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, specify 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 skills and training, and where appropriate certifications, required from the suppliers' or service providers' employees; (c) requirements regarding background checks of the suppliers' and service providers' employees pursuant to point 10.2; (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) provisions on repair times; (f) the right to audit or right to receive audit reports; EN 10 EN (g) 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; (h) 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); (i) 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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
16			**Application Software Security**								
16.1	Documentation	Govern	Establish and Maintain a Secure Application Development Process		x	x	Subset	6.2	Secure development life cycle	6.2.1	The relevant entities shall lay down, implement and apply rules for the secure development of network and information systems, including software, and apply them when acquiring or developing network and information systems. The rules shall cover all development phases, including specification, design, development, implementation and testing.
16.1	Documentation	Govern	Establish and Maintain a Secure Application Development Process		x	x	Subset	6.2	Secure development life cycle	6.2.2	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 information; EN 12 EN (f) sanitise and anonymize testing data according to the risk assessment.
16.1	Documentation	Govern	Establish and Maintain a Secure Application Development Process		x	x	Subset	6.2	Secure development life cycle	6.2.3	For outsourced development and procurement of network and information systems, the relevant entities shall apply the policies and procedures referred to in points 5 and 6.1.
16.1	Documentation	Govern	Establish and Maintain a Secure Application Development Process		x	x	Subset	6.2	Secure development life cycle	6.2.4	The relevant entities shall review and, where appropriate, update their secure development rules at planned intervals.
16.2	Documentation	Govern	Establish and Maintain a Process to Accept and Address Software Vulnerabilities		x	x					
16.3	Software	Protect	Perform Root Cause Analysis on Security Vulnerabilities		x	x					

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
16.4	Software	Identify	Establish and Manage an Inventory of Third-Party Software Components		x	x					
16.5	Software	Protect	Use Up-to-Date and Trusted Third-Party Software Components		x	x					
16.6	Documentation	Govern	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		x	x					
16.7	Software	Protect	Use Standard Hardening Configuration Templates for Application Infrastructure		x	x					
16.8	Network	Protect	Separate Production and Non-Production Systems		x	x					
16.9	Users	Protect	Train Developers in Application Security Concepts and Secure Coding		x	x					
16.10	Software	Protect	Apply Secure Design Principles in Application Architectures		x	x	Subset	6.2	Secure development life cycle	6.2.2	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 information; (f) sanitise and anonymize testing data according to the risk assessment.
16.11	Software	Protect	Leverage Vetted Modules or Services for Application Security Components		x	x					

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
16.12	Software	Protect	Implement Code-Level Security Checks			x					
16.13	Software	Detect	Conduct Application Penetration Testing			x					
16.14	Software	Protect	Conduct Threat Modelling			x					
17			**Incident Response Management**								
17.1	Users	Respond	Designate Personnel to Manage Incident Handling	x	x	x					
17.2	Documentation	Govern	Establish and Maintain Contact Information for Reporting Security Incidents	x	x	x	Subset	3.5	Incident 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.
17.3	Documentation	Govern	Establish and Maintain an Enterprise Process for Reporting Incidents	x	x	x	Subset	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.
17.3	Documentation	Govern	Establish and Maintain an Enterprise Process for Reporting Incidents	x	x	x	Subset	3.5	Incident 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.
17.4	Documentation	Govern	Establish and Maintain an Incident Response Process		x	x	Subset	3.5	Incident response	3.5.1	The relevant entities shall respond to incidents in accordance with documented procedures and in a timely manner.
17.4	Documentation	Govern	Establish and Maintain an Incident Response Process		x	x	Subset	3.5	Incident response	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.
17.4	Documentation	Govern	Establish and Maintain an Incident Response Process		x	x	Subset	3.5	Incident response	3.5.4	The relevant entities shall log incident response activities, and record evidence.
17.5	Users	Respond	Assign Key Roles and Responsibilities		x	x					

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
17.6	Users	Respond	Define Mechanisms for Communicating During Incident Response		x	x	Subset	3.5	Incident 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.
17.7	Users	Recover	Conduct Routine Incident Response Exercises		x	x	Equivalent	3.5	Incident response	3.5.5	The relevant entities shall test at planned intervals their incident response procedures.
17.8	Users	Recover	Conduct Post-Incident Reviews		x	x	Equivalent	3.6	Post-incident reviews	3.6.1	The relevant entities shall carry out post-incident reviews that shall identify the root cause of the incident and result in lessons learned to reduce the occurrence and consequences of future incidents.
17.8	Users	Recover	Conduct Post-Incident Reviews		x	x	Superset	3.6	Post-incident reviews	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.
17.8	Users	Recover	Conduct Post-Incident Reviews		x	x	Superset	3.6	Post-incident reviews	3.6.3	The relevant entities shall review at planned intervals if significant incidents led to post-incident reviews.
17.9	Documentation	Recover	Establish and Maintain Security Incident Thresholds			x	Subset	3.4	Event assessment and classifica-tion	3.4.1	The relevant entities shall assess suspicious events to determine whether they constitute incidents and, if so, determine their nature and severity.
17.9	Documentation	Recover	Establish and Maintain Security Incident Thresholds			x	Subset	3.4	Event assessment and classification	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 prioritization 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.

Control Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	NIS2 Relationship	NIS 2 Provision	NIS 2 Requirement Category	NIS2 Requirement #	NIS 2 Requirement Description
18			**Penetration Testing**								
18.1	Documentation	Govern	Establish and Maintain a Penetration Testing Program		x	x	Subset	6.5	Security testing	6.5.1	The relevant entities shall establish, implement and apply a policy and procedures for security testing.
18.1	Documentation	Govern	Establish and Maintain a Penetration Testing Program		x	x	Subset	6.5	Security testing	6.5.2	The relevant entities shall: (a) establish, based on the risk assessment, 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.
18.2	Network	Detect	Perform Periodic External Penetration Tests		x	x					
18.3	Network	Protect	Remediate Penetration Test Findings		x	x					
18.4	Network	Protect	Validate Security Measures			x					
18.5	Network	Detect	Perform Periodic Internal Penetration Tests			x					

Annex A:
Unmapped NIS2 Provisions

The following NIS2 Directive provisions NOT mapped to the Critical Security Controls Safeguards.

Table A.1

Directive Requirement#	Directive Provision
1.1.1	Policy on the security of network and information systems
1.1.2	Policy on the security of network and information systems
1.2.1	Roles, responsibilities and authorities
1.2.3	Roles, responsibilities and authorities
1.2.4	Roles, responsibilities and authorities
1.2.5	Roles, responsibilities and authorities
2.1.1	Risk management framework
2.1.2	Risk management framework
2.1.3	Risk management framework
2.2.1	Compliance monitoring
2.2.2	Compliance monitoring
2.2.3	Compliance monitoring
2.3.1	Independent review of information and network security
2.3.2	Independent review of information and network security
2.3.3	Independent review of information and network security
2.3.4	Independent review of information and network security
3.1.1	Incident handling policy
3.1.2	Incident handling policy
3.1.3	Incident handling policy
4.1.1	Business continuity and disaster recovery plans
4.1.2	Business continuity and disaster recovery plans
4.1.3	Business continuity and disaster recovery plans
4.1.4	Business continuity and disaster recovery plans
4.2.5	Backup management
4.3.1	Crisis management
4.3.2	Crisis management
4.3.3	Crisis management
4.3.4	Crisis management
5.1.3	Supply chain security policy
6.4.1	Change management, repairs and maintenance
6.4.2	Change management, repairs and maintenance
6.4.3	Change management, repairs and maintenance
6.4.4	Change management, repairs and maintenance
6.5.3	Security testing
6.8.3	Network segmentation
7.1.1	Policies and procedures
7.1.2	Policies and procedures
7.1.3	Policies and procedures
9.1.2	Cryptography
9.1.3	Cryptography
10.1.1	Human resources security
10.1.2	Human resources security
10.1.3	Human resources security
10.2.1	Background checks
10.2.2	Background checks
10.2.3	Background checks
10.3.1	Termination or change of employment procedures
10.4.1	Termination or change of employment procedures
10.4.2	Termination or change of employment procedures
11.1.2	Access control policy
11.1.3	Access control policy
11.3.1	Privileged accounts and system administration accounts
11.5.2	Identification

Directive Requirement#	Directive Provision
11.5.3	Identification
12.3.3	Removable media policy
12.5.1	Return or deletion of assets upon termination of employment
13.1.1	Supporting utilities
13.1.2	Supporting utilities
13.1.3	Supporting utilities
13.2.1	Protection against physical and environmental threats
13.2.2	Protection against physical and environmental threats
13.2.3	Protection against physical and environmental threats
13.3.1	Perimeter and physical access control
13.3.2	Perimeter and physical access control
13.3.3	Perimeter and physical access control

Annex B:
Unmapped Critical Security Control Safeguards

The following Critical Security Controls Safeguards are NOT mapped to the NIS2 Directive provisions

Table B.1

Safeguard	Safeguard Name
1.2	Address Unauthorized Assets
1.3	Utilize an Active Discovery Tool
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory
1.5	Use a Passive Asset Discovery Tool
2.1	Establish and Maintain a Software Inventory
2.3	Address Unauthorized Software
2.4	Utilize Automated Software Inventory Tools
2.5	Allowlist Authorized Software
2.6	Allowlist Authorized Libraries
2.7	Allowlist Authorized Scripts
3.2	Establish and Maintain a Data Inventory
3.4	Enforce Data Retention
3.8	Document Data Flows
3.1	Encrypt Sensitive Data in Transit
3.1	Encrypt Sensitive Data at Rest
3.1	Deploy a Data Loss Prevention Solution
4.4	Implement and Manage a Firewall on Servers
4.5	Implement and Manage a Firewall on End-User Devices
4.6	Securely Manage Enterprise Assets and Software
4.7	Manage Default Accounts on Enterprise Assets and Software
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
4.9	Configure Trusted DNS Servers on Enterprise Assets
4.1	Enforce Remote Wipe Capability on Portable End-User Devices
4.1	Separate Enterprise Workspaces on Mobile End-User Devices
5.2	Use Unique Passwords
5.3	Disable Dormant Accounts
5.5	Establish and Maintain an Inventory of Service Accounts
5.6	Centralize Account Management
7.3	Perform Automated Operating System Patch Management
7.4	Perform Automated Application Patch Management
8.3	Ensure Adequate Audit Log Storage
8.6	Collect DNS Query Audit Logs
8.7	Collect URL Request Audit Logs
8.8	Collect Command-Line Audit Logs
8.1	Collect Service Provider Logs
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients
9.3	Maintain and Enforce Network-Based URL Filters
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions
9.6	Block Unnecessary File Types
9.7	Deploy and Maintain Email Server Anti-Malware Protections
10	Configure Automatic Anti-Malware Signature Updates
11	Enable Anti-Exploitation Features
11	Centrally Manage Anti-Malware Software
11	Use Behaviour-Based Anti-Malware Software
11	Perform Automated Backups
12	Securely Manage Network Infrastructure
13	Centralize Network Authentication, Authorization, and Auditing (AAA)
13	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure
13	Centralize Security Event Alerting
13	Deploy a Host-Based Intrusion Detection Solution
13	Perform Traffic Filtering Between Network Segments
14	Manage Access Control for Remote Assets
14	Collect Network Traffic Flow Logs
14	Deploy a Host-Based Intrusion Prevention Solution
14	Deploy a Network Intrusion Prevention Solution

Safeguard	Safeguard Name
14	Deploy Port-Level Access Control
13	Perform Application Layer Filtering
14	Train Workforce Members to Recognize Social Engineering Attacks
14	Train Workforce Members on Authentication Best Practices
14	Train Workforce on Data Handling Best Practices
15	Train Workforce Members on Causes of Unintentional Data Exposure
15	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
15	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
15	Classify Service Providers
16	Establish and Maintain a Process to Accept and Address Software Vulnerabilities
16	Perform Root Cause Analysis on Security Vulnerabilities
16	Establish and Manage an Inventory of Third-Party Software Components
17	Use Up-to-Date and Trusted Third-Party Software Components
17	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities
17	Use Standard Hardening Configuration Templates for Application Infrastructure
17	Separate Production and Non-Production Systems
17	Train Developers in Application Security Concepts and Secure Coding
16	Leverage Vetted Modules or Services for Application Security Components
16	Implement Code-Level Security Checks
16	Conduct Application Penetration Testing
16	Conduct Threat Modelling
17	Designate Personnel to Manage Incident Handling
18	Assign Key Roles and Responsibilities
18	Perform Periodic External Penetration Tests
18	Remediate Penetration Test Findings
18	Validate Security Measures
19	Perform Periodic Internal Penetration Tests

History

Document history		
V1.1.1	September 2025	Publication