ETSI TR 104 169 V1.1.1 (2025-09)

TECHNICAL REPORT

Cyber Security (CYBER);
Critical Security Controls for
the Digital Operational Resilience Act (DORA)

Reference
DTR/CYBER-00157

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 DORA 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 DORA 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 provides a mapping between the Critical Security Controls and DORA 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] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[i.2] 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.3] 2020/0266 (COD), COM(2020) 595 final: "Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014".

[i.4] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[i.5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.6] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[i.7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[i.8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.9] Center for Internet Security: "CIS Controls v8.1 Mapping to DORA".

[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 103 960: "Cyber Security (CYBER); Implementation of the Digital Operational Resilience Act (DORA)".

[i.15] NIST CSF PR.DS-7: "The development and testing environment(s) are separate from the production environment".

[i.16] NIST CSF PR.DS-3: "Assets are formally managed throughout removal, transfers, and disposition".

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:

AAA	Authentication, Authorization, and Accounting
COTS	Commercial Off The Shelf
CSC	Critical Security Controls
CSF	Computer Security Framework
DHCP	Dynamic Host Configuration Protocol
DORA	Digital Operational Resilience Act
ERM	Enterprise Risk Management
IG1	Implementation Group 1
IG2	Implementation Group 2
IG3	Implementation Group 3
SSO	Single Sign-On

4 Applying the Critical Security Controls for effective implementation of DORA

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 DORA. 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 DORA 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 DORA 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 [i.15].
- Safeguard 3.5 "Securely Dispose of Data" is a subset of NIST CSF PR.DS-3 [i.16].

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 [i.10] 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.

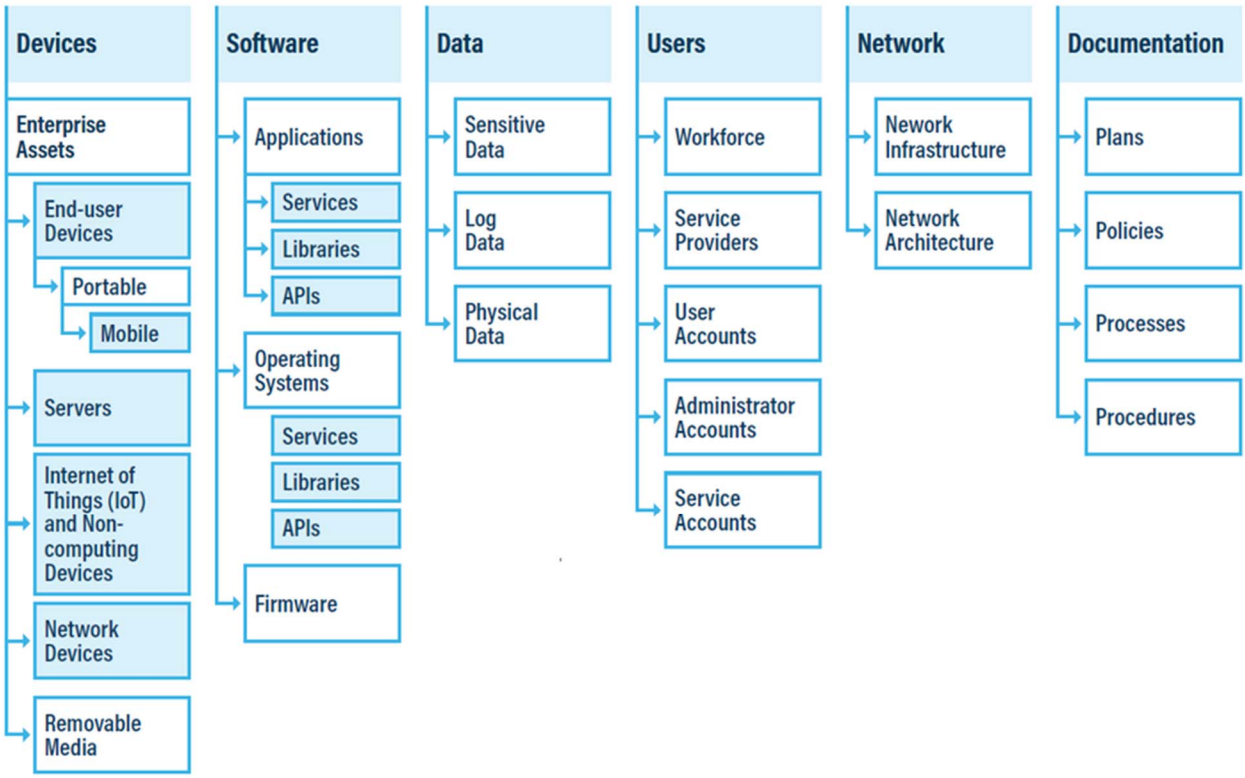

Figure 4.1-1

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 is required by DORA to 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 is required by DORA to abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

4.2 Applicability Overview

Table 4.2-1 below provides a mapping by the Critical Security Controls community to the DORA provisions to support the indicated requirements [i.9].

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

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	8 of 14
4	Secure Configuration of Enterprise Assets and Software	0 of 12
5	Account Management	0 of 6
6	Access Control Management	3 of 8
7	Continuous Vulnerability Management	2 of 9
8	Audit Log Management	0 of 12
9	Email and Web Browser Protections	0 of 7
10	Malware Defences	0 of 7
11	Data Recovery	4 of 5
12	Network Infrastructure Management	1 of 8
13	Network Monitoring and Defence	5 of 11

Control	Safeguard Title	Applicability
14	Security Awareness and Skills Training	2 of 9
15	Service Provider Management	6 of 7
16	Application Software Security	0 of 14
17	Incident Response Management	7 of 9
18	Penetration Testing	0 of 5

4.3 Applying the Critical Security Controls and Safeguards

Table 4.3-1

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
1			**Inventory and Control of Enterprise Assets**							
1.1	Devices	**Identify**	Establish and Maintain Detailed Enterprise Asset Inventory	x	x	x	Subset	8.1	Identification	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.
1.1	Devices	**Identify**	Establish and Maintain Detailed Enterprise Asset Inventory	x	x	x	Subset	8.4	Identification	Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and shall map those considered critical. They shall map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.
1.1	Devices	**Identify**	Establish and Maintain Detailed Enterprise Asset Inventory	x	x	x	Subset	8.6	Identification	For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in paragraph 3 occurs.
1.2	Devices	**Respond**	Address Unauthorized Assets	x	x	x				
1.3	Devices	**Detect**	Utilize an Active Discovery Tool		x	x				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
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	Subset	8.1	Identification	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.
2.1	Software	Identify	Establish and Maintain a Software Inventory	x	x	x	Subset	8.6	Identification	For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in 3 occurs.
2.2	Software	Identify	Ensure Authorized Software is Currently Supported	x	x	x				
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	Subset	9.3, Point (d)	Protection and Prevention	Ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
3.1	Data	Govern	Establish and Maintain a Data Management Process	x	x	x	Subset	9.4, Point (a)	Protection and Prevention	Develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers, where applicable.
3.2	Data	Identify	Establish and Maintain a Data Inventory	x	x	x	Subset	8.1	Identification	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.
3.2	Data	Identify	Establish and Maintain a Data Inventory	x	x	x	Subset	8.6	Identification	For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in 3 occurs.
3.3	Data	Protect	Configure Data Access Control Lists	x	x	x				
3.4	Data	Protect	Enforce Data Retention	x	x	x				
3.5	Data	Protect	Securely Dispose of Data	x	x	x				
3.6	Data	Protect	Encrypt Data on End-User Devices	x	x	x				
3.7	Data	Identify	Establish and Maintain a Data Classification Scheme		x	x	Subset	9.4, Point (d)	Protection and Prevention	Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
3.8	Data	Identify	Document Data Flows		x	x	Subset	8.4	Identification	Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and shall map those considered critical. They shall map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.
3.8	Data	Identify	Document Data Flows		x	x	Subset	8.6	Identification	For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in 3 occurs.
3.9	Data	Protect	Encrypt Data on Removable Media		x	x				
3.10	Data	Protect	Encrypt Sensitive Data in Transit		x	x	Subset	9.3, Point (a)	Protection and Prevention	Ensure the security of the means of transfer of data.
3.11	Data	Protect	Encrypt Sensitive Data at Rest		x	x	Subset	9.3, Point (b)	Protection and Prevention	Minimize the risk of corruption or loss of data, unauthorized access and technical flaws that may hinder business activity.
3.12	Data	Protect	Segment Data Processing and Storage Based on Sensitivity		x	x	Subset	9.4, Point (b)	Protection and Prevention	Following a risk-based approach, establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks.
3.13	Data	Protect	Deploy a Data Loss Prevention Solution			x	Subset	9.3, Point (b)	Protection and Prevention	Minimize the risk of corruption or loss of data, unauthorized access and technical flaws that may hinder business activity.
3.13	Data	Protect	Deploy a Data Loss Prevention Solution			x	Subset	9.3, Point (c)	Protection and Prevention	Prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data.
3.14	Data	Detect	Log Sensitive Data Access			x				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
4			**Secure Configuration of Enterprise Assets and Software**							
4.1	Documentation	Govern	Establish and Maintain a Secure Configuration Process	x	x	x				
4.2	Documentation	Govern	Establish and Maintain a Secure Configuration Process for Network Infrastructure	x	x	x				
4.3	Devices	Protect	Configure Automatic Session Locking on Enterprise Assets	x	x	x				
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				
4.10	Devices	Protect	Enforce Automatic Device Lockout on Portable End-User Devices		x	x				
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				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
5			**Account Management**							
5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	x	x	x				
5.2	Users	Protect	Use Unique Passwords	x	x	x				
5.3	Users	Protect	Disable Dormant Accounts	x	x	x				
5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	x	x	x				
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**							
6.1	Documentation	Govern	Establish an Access Granting Process	x	x	x				
6.2	Documentation	Govern	Establish an Access Revoking Process	x	x	x				
6.3	Users	Protect	Require MFA for Externally-Exposed Applications	x	x	x				
6.4	Users	Protect	Require MFA for Remote Network Access	x	x	x				
6.5	Users	Protect	Require MFA for Administrative Access	x	x	x				
6.6	Software	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems		x	x	Subset	9.4, Point (d)	Protection and Prevention	Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes.
6.7	Users	Protect	Centralize Access Control		x	x	Subset	9.4, Point (d)	Protection and Prevention	Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
6.8	Users	Govern	Define and Maintain Role-Based Access Control			x	Subset	5.2, Point (c)	Governance and Organization	Set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions.
6.8	Users	Govern	Define and Maintain Role-Based Access Control			x	Subset	8.1	Identification	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.
6.8	Users	Govern	Define and Maintain Role-Based Access Control			x	Subset	8.6	Identification	For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in 3 occurs.
6.8	Users	Govern	Define and Maintain Role-Based Access Control			x	Subset	9.4, Point (c)	Protection and Prevention	Implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
7			**Continuous Vulnerability Management**							
7.1	Documentation	Govern	Establish and Maintain a Vulnerability Management Process	x	x	x	Subset	9.1	Protection and Prevention	For the purposes of adequately protecting ICT systems and with a view to organizing response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimize the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures.
7.1	Documentation	Govern	Establish and Maintain a Vulnerability Management Process	x	x	x	Subset	9.4, Point (f)	Protection and Prevention	Have appropriate and comprehensive documented policies for patches and updates.
7.1	Documentation	Govern	Establish and Maintain a Vulnerability Management Process	x	x	x	Subset	16.1, Point (c)	Simplified ICT Risk Management Framework	Minimize the impact of ICT risk through the use of sound, resilient and updated ICT systems, protocols and tools which are appropriate to support the performance of their activities and the provision of services and adequately protect availability, authenticity, integrity and confidentiality of data in the network and information systems.
7.1	Documentation	Govern	Establish and Maintain a Vulnerability Management Process	x	x	x	Subset	16.1, Point (d)	Simplified ICT Risk Management Framework	Allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and detected and ICT-related incidents to be swiftly handled.
7.2	Documentation	Govern	Establish and Maintain a Remediation Process	x	x	x	Subset	9.4, Point (f)	Protection and Prevention	Have appropriate and comprehensive documented policies for patches and updates.
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				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
7.6	Software	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		x	x				
7.7	Software	Respond	Remediate Detected Vulnerabilities		x	x				
8			**Audit Log Management**							
8.1	Documentation	Govern	Establish and Maintain an Audit Log Management Process	x	x	x				
8.2	Data	Detect	Collect Audit Logs	x	x	x				
8.3	Data	Protect	Ensure Adequate Audit Log Storage	x	x	x				
8.4	Network	Protect	Standardize Time Synchronization		x	x				
8.5	Data	Detect	Collect Detailed Audit Logs		x	x				
8.6	Data	Detect	Collect DNS Query Audit Logs		x	x				
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				
8.10	Data	Protect	Retain Audit Logs		x	x				
8.11	Data	Detect	Conduct Audit Log Reviews		x	x				
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				
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				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
9.5	Network	Protect	Implement DMARC		x	x				
9.6	Network	Protect	Block Unnecessary File Types		x	x				
9.7	Network	Protect	Deploy and Maintain Email Server Anti-Malware Protections			x				
10			**Malware Defenses**							
10.1	Devices	Detect	Deploy and Maintain Anti-Malware Software	x	x	x				
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				
10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media		x	x				
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	Equivalent	12.1, Point (a)	Backup and Restoration	Backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data.
11.1	Documentation	Govern	Establish and Maintain a Data Recovery Process	x	x	x	Superset	12.1, Point (b)	Backup and Restoration	Restoration and recovery procedures and methods.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
11.1	Documentation	Govern	Establish and Maintain a Data Recovery Process	x	x	x	Superset	12.2	Backup and Restoration	Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. The activation of backup systems shall not jeopardize the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically.
11.1	Documentation	Govern	Establish and Maintain a Data Recovery Process	x	x	x	Superset	16.1, Point (f)	Simplified ICT Risk Management Framework	Ensure the continuity of critical or important functions, through business continuity plans and response and recovery measures, which include, at least, back-up and restoration measures.
11.2	Data	Recover	Perform Automated Backups	x	x	x				
11.3	Data	Protect	Protect Recovery Data	x	x	x	Subset	12.7	Backup and Restoration	When recovering from an ICT-related incident, financial entities shall perform necessary checks, including any multiple checks and reconciliations, in order to ensure that the highest level of data integrity is maintained. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
11.4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data	x	x	x	Subset	12.3	Backup and Restoration	When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system. The ICT systems shall be securely protected from any unauthorized access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary. For central counterparties, the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date. Data reporting service providers shall additionally maintain adequate resources and have back-up and restoration facilities in place in order to offer and maintain their services at all times.
11.5	Data	Recover	Test Data Recovery		x	x	Subset	12.2	Backup and Restoration	Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. The activation of backup systems shall not jeopardize the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically.
11.5	Data	Recover	Test Data Recovery		x	x	Subset	16.1, Point (g)	Simplified ICT Risk Management Framework	Test, on a regular basis, the plans and measures referred to in point (f), as well as the effectiveness of the controls implemented in accordance with points (a) and (c).

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
12			**Network Infrastructure Management**							
12.1	Network	**Protect**	Ensure Network Infrastructure is Up-to-Date	x	x	x				
12.2	Network	**Protect**	Establish and Maintain a Secure Network Architecture		x	x	Subset	5.2, Point (b)	Governance and Organization	Put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data.
12.2	Network	**Protect**	Establish and Maintain a Secure Network Architecture		x	x	Subset	9.4, Point (b)	Protection and Prevention	Following a risk-based approach, establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks.
12.3	Network	**Protect**	Securely Manage Network Infrastructure		x	x				
12.4	Documentation	**Govern**	Establish and Maintain Architecture Diagram(s)		x	x				
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				
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				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
13			**Network Monitoring and Defense**							
13.1	Network	**Detect**	Centralize Security Event Alerting		x	x	Subset	10.1	Detection	Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure. All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 25.
13.1	Network	**Detect**	Centralize Security Event Alerting		x	x	Subset	16.1, Point (b)	Simplified ICT Risk Management Framework	Continuously monitor the security and functioning of all ICT systems.
13.2	Devices	**Detect**	Deploy a Host-Based Intrusion Detection Solution		x	x	Subset	9.1	Protection and Prevention	For the purposes of adequately protecting ICT systems and with a view to organizing response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimize the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures.
13.2	Devices	**Detect**	Deploy a Host-Based Intrusion Detection Solution		x	x	Subset	10.1	Detection	Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure. All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 25.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
13.2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution		x	x	Subset	10.3	Detection	Financial entities shall devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution		x	x	Subset	10.1	Detection	Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure. All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 25.
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	Subset	10.2	Detection	The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.
13.6	Network	Detect	Collect Network Traffic Flow Logs		x	x	Subset	10.3	Detection	Financial entities shall devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.
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				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
13.11	Network	Detect	Tune Security Event Alerting Thresholds			x	Subset	10.2	Detection	The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.
14			**Security Awareness and Skills Training**							
14.1	Documentation	Govern	Establish and Maintain a Security Awareness Program	x	x	x	Superset	13.6	Learning and Evolving	Financial entities shall develop ICT security awareness programmes and digital operational resilience training as compulsory modules in their staff training schemes. Those programmes and training shall be applicable to all employees and to senior management staff, and shall have a level of complexity commensurate to the remit of their functions. Where appropriate, financial entities shall also include ICT third-party service providers in their relevant training schemes in accordance with Article 30(2), point (i).
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				
14.7	Users	Protect	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	x	x	x				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
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	5.4	Governance and Organization	Members of the management body of the financial entity shall actively keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risk being managed.
15			**Service Provider Management**							
15.1	Users	Identify	Establish and Maintain an Inventory of Service Providers	x	x	x	Subset	8.5	Identification	Financial entities shall identify and document all processes that are dependent on ICT third-party service providers, and shall identify interconnections with ICT third-party service providers that provide services that support critical or important functions.
15.1	Users	Identify	Establish and Maintain an Inventory of Service Providers	x	x	x	Subset	8.6	Identification	For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in paragraph 3 occurs.
15.2	Documentation	Govern	Establish and Maintain a Service Provider Management Policy		x	x	Subset	5.2, Point (b)	Governance and Organization	put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data.
15.2	Documentation	Govern	Establish and Maintain a Service Provider Management Policy		x	x	Subset	5.2, Point (h)	Governance and Organization	Approve and periodically review the financial entity's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers. Put in place, at corporate level, reporting channels enabling it to be duly informed of the following.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
15.3	Users	Govern	Classify Service Providers		x	x	Subset	8.5	Identification	Financial entities shall identify and document all processes that are dependent on ICT third-party service providers, and shall identify interconnections with ICT third-party service providers that provide services that support critical or important functions.
15.3	Users	Govern	Classify Service Providers		x	x	Subset	8.6	Identification	For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in paragraph 3 occurs.
15.3	Users	Govern	Classify Service Providers		x	x	Subset	16.1, Point (e)	Simplified ICT Risk Management Framework	Identify key dependencies on ICT third-party service providers.
15.4	Documentation	Govern	Ensure Service Provider Contracts Include Security Requirements		x	x	Subset	5.2, Point (h), Subpoint (ii)	Governance and Organization	The potential impact of such changes on the critical or important functions subject to those arrangements, including a risk analysis summary to assess the impact of those changes, and at least major ICT-related incidents and their impact, as well as response, recovery and corrective measures.
15.4	Documentation	Govern	Ensure Service Provider Contracts Include Security Requirements		x	x	Subset	10.4	Detection	Data reporting service providers shall, in addition, have in place systems that can effectively check trade reports for completeness, identify omissions and obvious errors, and request re-transmission of those reports.
15.5	Users	Govern	Assess Service Providers			x				
15.6	Data	Govern	Monitor Service Providers			x	Subset	5.2, Point (h), Subpoint (ii)	Governance and Organization	Any relevant planned material changes regarding the ICT third-party service providers.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
15.6	Data	Govern	Monitor Service Providers			x	Subset	5.3	Governance and Organization	Financial entities, other than microenterprises, shall establish a role in order to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or shall designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.
15.7	Data	Protect	Securely Decommission Service Providers			x	Superset	5.2, Point (h), Subpoint (i)	Governance and Organization	Arrangements concluded with ICT third-party service providers on the use of ICT services.
16			**Application Software Security**							
16.1	Documentation	Govern	Establish and Maintain a Secure Application Development Process		x	x				
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				
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				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
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				
16.11	Software	Protect	Leverage Vetted Modules or Services for Application Security Components		x	x				
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	Subset	5.2, Point (c)	Governance and Organization	Set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions.
17.1	Users	Respond	Designate Personnel to Manage Incident Handling	x	x	x	Superset	14.3	Communication	At least one person in the financial entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfil the public and media function for that purpose.
17.1	Users	Respond	Designate Personnel to Manage Incident Handling	x	x	x	Superset	17.3, Point (c)	ICT-related incident management process	Assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios.
17.2	Documentation	Govern	Establish and Maintain Contact Information for Reporting Security Incidents	x	x	x	Subset	11.2, Point (e)	Response and Recovery	Set out communication and crisis management actions that ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 14, and report to the competent authorities in accordance with Article 19.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
17.2	Documentation	Govern	Establish and Maintain Contact Information for Reporting Security Incidents	x	x	x	Subset	14.1	Communication	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.
17.2	Documentation	Govern	Establish and Maintain Contact Information for Reporting Security Incidents	x	x	x	Subset	17.3, Point (d)	ICT-related incident management process	Set out plans for communication to staff, external stakeholders and media in accordance with Article 14 and for notification to clients, for internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate.
17.2	Documentation	Govern	Establish and Maintain Contact Information for Reporting Security Incidents	x	x	x	Subset	17.3, Point (e)	ICT-related incident management process	Ensure that at least major ICT-related incidents are reported to relevant senior management and inform the management body of at least major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of such ICT-related incidents.
17.2	Documentation	Govern	Establish and Maintain Contact Information for Reporting Security Incidents	x	x	x	Subset	19.1	Reporting of major ICT-related incidents and voluntary notification of significant cyber threats	Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 in accordance with paragraph 4 of this Article.
17.3	Documentation	Govern	Establish and Maintain an Enterprise Process for Reporting Incidents	x	x	x				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
17.4	Documentation	Govern	Establish and Maintain an Incident Response Process		x	x	Subset	5.2, Point (e)	Governance and Organization	Approve, oversee and periodically review the implementation of the financial entity's ICT business continuity policy and ICT response and recovery plans, referred to, respectively, in Article 11(1) and (3), which may be adopted as a dedicated specific policy forming an integral part of the financial entity's overall business continuity policy and response and recovery plan.
17.4	Documentation	Govern	Establish and Maintain an Incident Response Process		x	x	Subset	11.2, Point (b)	Response and Recovery	Quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritizes the resumption of activities and recovery actions.
17.4	Documentation	Govern	Establish and Maintain an Incident Response Process		x	x	Subset	11.2, Point (c)	Response and Recovery	Activate, without delay, dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and prevent further damage, as well as tailored response and recovery procedures established in accordance with Article 12.
17.4	Documentation	Govern	Establish and Maintain an Incident Response Process		x	x	Subset	16.1, Point (f)	Simplified ICT Risk Management Framework	Ensure the continuity of critical or important functions, through business continuity plans and response and recovery measures, which include, at least, back-up and restoration measures.
17.4	Documentation	Govern	Establish and Maintain an Incident Response Process		x	x	Subset	17.1	ICT-related incident management process	Financial entities shall define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.
17.4	Documentation	Govern	Establish and Maintain an Incident Response Process		x	x	Subset	17.2	ICT-related incident management process	Financial entities shall record all ICT-related incidents and significant cyber threats. Financial entities shall establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
17.4	Documentation	Govern	Establish and Maintain an Incident Response Process		x	x	Subset	17.3, Point (f)	ICT-related incident management process	Establish ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner.
17.5	Users	Respond	Assign Key Roles and Responsibilities		x	x				
17.6	Users	Respond	Define Mechanisms for Communicating During Incident Response		x	x	Subset	11.2, Point (e)	Response and Recovery	Set out communication and crisis management actions that ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 14, and report to the competent authorities in accordance with Article 19.
17.6	Users	Respond	Define Mechanisms for Communicating During Incident Response		x	x	Subset	11.6, Point (b)	Response and Recovery	Test the crisis communication plans established in accordance with Article 14.
17.6	Users	Respond	Define Mechanisms for Communicating During Incident Response		x	x	Subset	11.7	Response and Recovery	Financial entities, other than microenterprises, shall have a crisis management function, which, in the event of activation of their ICT business continuity plans or ICT response and recovery plans, shall, inter alia, set out clear procedures to manage internal and external crisis communications in accordance with Article 14.
17.7	Users	Recover	Conduct Routine Incident Response Exercises		x	x	Subset	11.4	Response and Recovery	Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.
17.7	Users	Recover	Conduct Routine Incident Response Exercises		x	x	Subset	11.6, Point (a)	Response and Recovery	Test the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least yearly, as well as in the event of any substantive changes to ICT systems supporting critical or important functions.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
17.7	Users	Recover	Conduct Routine Incident Response Exercises		x	x	Subset	16.1, Point (g)	Simplified ICT Risk Management Framework	Test, on a regular basis, the plans and measures referred to in point (f), as well as the effectiveness of the controls implemented in accordance with points (a) and (c).
17.8	Users	Recover	Conduct Post-Incident Reviews		x	x	Subset	13.1	Learning and Evolving	Financial entities shall have in place capabilities and staff to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse the impact they are likely to have on their digital operational resilience.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
17.8	Users	**Recover**	Conduct Post-Incident Reviews		x	x	Subset	13.2	Learning and Evolving	Financial entities shall put in place post ICT-related incident reviews after a major ICT-related incident disrupts their core activities, analysing the causes of disruption and identifying required improvements to the ICT operations or within the ICT business continuity policy referred to in Article 11. Financial entities, other than microenterprises, shall, upon request, communicate to the competent authorities, the changes that were implemented following post ICT-related incident reviews as referred to in the first subparagraph. The post ICT-related incident reviews referred to in the first subparagraph shall determine whether the established procedures were followed and the actions taken were effective, including in relation to the following: (a) the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity; (b) the quality and speed of performing a forensic analysis, where deemed appropriate; (c) the effectiveness of incident escalation within the financial entity; (d) the effectiveness of internal and external communication.

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
17.8	Users	Recover	Conduct Post-Incident Reviews		x	x	Subset	13.3	Learning and Evolving	Lessons derived from the digital operational resilience testing carried out in accordance with Articles 26 and 27 and from real life ICT-related incidents, in particular cyber-attacks, along with challenges faced upon the activation of ICT business continuity plans and ICT response and recovery plans, together with relevant information exchanged with counterparts and assessed during supervisory reviews, shall be duly incorporated on a continuous basis into the ICT risk assessment process. Those findings shall form the basis for appropriate reviews of relevant components of the ICT risk management framework referred to in Article 6(1).
17.9	Documentation	Recover	Establish and Maintain Security Incident Thresholds			x	Subset	10.2	Detection	The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.
17.9	Documentation	Recover	Establish and Maintain Security Incident Thresholds			x	Superset	17.3, Point (a)	ICT-related incident management process	Put in place early warning indicators.
17.9	Documentation	Recover	Establish and Maintain Security Incident Thresholds			x	Superset	17.3, Point (b)	ICT-related incident management process	Establish procedures to identify, track, log, categorize and classify ICT-related incidents according to their priority and severity and according to the criticality of the services impacted, in accordance with the criteria set out in Article 18(1).
18			**Penetration Testing**							
18.1	Documentation	Govern	Establish and Maintain a Penetration Testing Program		x	x				
18.2	Network	Detect	Perform Periodic External Penetration Tests		x	x				

CIS Safeguard	Control Asset Type	Safeguard Security Function	Control / Safeguard Title	IG1	IG2	IG3	DORA Relationship	DORA Provision	DORA Category	DORA Requirement Description
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 DORA Provisions

The following DORA provisions are NOT mapped to the Critical Security Controls Safeguards.

Table A.1

DORA Requirement #	DORA Provision
5.1	Governance and Organization
5.2	Governance and Organization
5.2(a)	Governance and Organization
5.2(d)	Governance and Organization
5.2(f)	Governance and Organization
5.2(g)	Governance and Organization
6.1	ICT Risk Management Framework
6.2	ICT Risk Management Framework
6.3	ICT Risk Management Framework
6.4	ICT Risk Management Framework
6.5	ICT Risk Management Framework
6.6	ICT Risk Management Framework
6.7	ICT Risk Management Framework
6.8	ICT Risk Management Framework
6.8(a)	ICT Risk Management Framework
6.8(b)	ICT Risk Management Framework
6.8(c)	ICT Risk Management Framework
6.8(d)	ICT Risk Management Framework
6.8(e)	ICT Risk Management Framework
6.8(f)	ICT Risk Management Framework
6.8(g)	ICT Risk Management Framework
6.8(h)	ICT Risk Management Framework
6.9	ICT Risk Management Framework
6.1	ICT Risk Management Framework
8.2	Identification
8.3	Identification
8.7	Identification
9.2	Protection and Prevention
9.3	Protection and Prevention
9.4	Protection and Prevention
9.4(e)	Protection and Prevention
11.1	Response and Recovery
11.2	Response and Recovery
11.2(a)	Response and Recovery
11.2(d)	Response and Recovery
11.3	Response and Recovery
11.5	Response and Recovery
11.6	Response and Recovery
11.8	Response and Recovery
11.9	Response and Recovery
11.1	Response and Recovery
11.11	Response and Recovery
12.1	Backup and Restoration
12.4	Backup and Restoration
12.5	Backup and Restoration
12.5(a)	Backup and Restoration
12.5(b)	Backup and Restoration
12.5(c)	Backup and Restoration
12.6	Backup and Restoration
13.4	Learning and Evolving
13.5	Learning and Evolving
13.7	Learning and Evolving
14.2	Communication

DORA Requirement #	DORA Provision
16.1(a)	Simplified ICT Risk Management Framework
16.1(h)	Simplified ICT Risk Management Framework
16.2	Simplified ICT Risk Management Framework
17.3	ICT-related incident management process

Annex B:
Unmapped Critical Security Control Safeguards

The following Critical Security Controls Safeguards are NOT mapping to DORA requirements.

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
2.2	Ensure Authorized Software is Currently Supported
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
3.3	Configure Data Access Control Lists
3.4	Enforce Data Retention
3.5	Securely Dispose of Data
3.6	Encrypt Data on End-User Devices
3.9	Encrypt Data on Removable Media
3.14	Log Sensitive Data Access
4.1	Establish and Maintain a Secure Configuration Process
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure
4.3	Configure Automatic Session Locking on Enterprise Assets
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 Automatic Device Lockout on Portable End-User Devices
4.11	Enforce Remote Wipe Capability on Portable End-User Devices
4.12	Separate Enterprise Workspaces on Mobile End-User Devices
5.1	Establish and Maintain an Inventory of Accounts
5.2	Use Unique Passwords
5.3	Disable Dormant Accounts
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts
5.5	Establish and Maintain an Inventory of Service Accounts
5.6	Centralize Account Management
6.1	Establish an Access Granting Process
6.2	Establish an Access Revoking Process
6.3	Require MFA for Externally-Exposed Applications
6.4	Require MFA for Remote Network Access
6.5	Require MFA for Administrative Access
7.3	Perform Automated Operating System Patch Management
7.4	Perform Automated Application Patch Management
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
7.7	Remediate Detected Vulnerabilities
8.1	Establish and Maintain an Audit Log Management Process
8.2	Collect Audit Logs
8.3	Ensure Adequate Audit Log Storage
8.4	Standardize Time Synchronization
8.5	Collect Detailed Audit Logs
8.6	Collect DNS Query Audit Logs
8.7	Collect URL Request Audit Logs
8.8	Collect Command-Line Audit Logs
8.9	Centralize Audit Logs
8.1	Retain Audit Logs
8.11	Conduct Audit Log Reviews

Safeguard	Safeguard Name
8.12	Collect Service Provider Logs
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients
9.2	Use DNS Filtering Services
9.3	Maintain and Enforce Network-Based URL Filters
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions
9.5	Implement DMARC
9.6	Block Unnecessary File Types
9.7	Deploy and Maintain Email Server Anti-Malware Protections
10.1	Deploy and Maintain Anti-Malware Software
10.2	Configure Automatic Anti-Malware Signature Updates
10.3	Disable Autorun and Autoplay for Removable Media
10.4	Configure Automatic Anti-Malware Scanning of Removable Media
10.5	Enable Anti-Exploitation Features
10.6	Centrally Manage Anti-Malware Software
10.7	Use Behaviour-Based Anti-Malware Software
11.2	Perform Automated Backups
12.1	Ensure Network Infrastructure is Up-to-Date
12.3	Securely Manage Network Infrastructure
12.4	Establish and Maintain Architecture Diagram(s)
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)
12.6	Use of Secure Network Management and Communication Protocols
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure
12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work
13.4	Perform Traffic Filtering Between Network Segments
13.5	Manage Access Control for Remote Assets
13.7	Deploy a Host-Based Intrusion Prevention Solution
13.8	Deploy a Network Intrusion Prevention Solution
13.9	Deploy Port-Level Access Control
13.1	Perform Application Layer Filtering
14.2	Train Workforce Members to Recognize Social Engineering Attacks
14.3	Train Workforce Members on Authentication Best Practices
14.4	Train Workforce on Data Handling Best Practices
14.5	Train Workforce Members on Causes of Unintentional Data Exposure
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
15.5	Assess Service Providers
16.1	Establish and Maintain a Secure Application Development Process
16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities
16.3	Perform Root Cause Analysis on Security Vulnerabilities
16.4	Establish and Manage an Inventory of Third-Party Software Components
16.5	Use Up-to-Date and Trusted Third-Party Software Components
16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities
16.7	Use Standard Hardening Configuration Templates for Application Infrastructure
16.8	Separate Production and Non-Production Systems
16.9	Train Developers in Application Security Concepts and Secure Coding
16.1	Apply Secure Design Principles in Application Architectures
16.11	Leverage Vetted Modules or Services for Application Security Components
16.12	Implement Code-Level Security Checks
16.13	Conduct Application Penetration Testing
16.14	Conduct Threat Modelling
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents
17.5	Assign Key Roles and Responsibilities
18.1	Establish and Maintain a Penetration Testing Program
18.2	Perform Periodic External Penetration Tests
18.3	Remediate Penetration Test Findings
18.4	Validate Security Measures
18.5	Perform Periodic Internal Penetration Tests

History

Document history		
V1.1.1	September 2025	Publication