ETSI TR 103 960 V1.1.1 (2025-05)

Cyber Security (CYBER);
Implementation of the
Digital Operational Resilience Act (DORA)

Reference
DTR/CYBER-00110

Keywords
cyber security, resilience, risk management

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 Digital Operational Resilience Act (DORA), came into effect on 16 January 2023, and focuses on the significant economic and systemic risk posed by the potential disruption of critical ICT systems, e.g. due to technical faults, operational error, or cybercrime, and becomes effective on 17 Jan 2025 [i.1]. It contains a broad range of measures aimed at improving the robustness of financial-sector ICT infrastructures, covering both in-house systems and services outsourced to third-party providers (TPPs). Twelve new mandates to issue eight technical standards, guidelines and reports were required in 2024. [Annex A] Concurrently with DORA, the Directive on Network and Information Security (NIS 2), the Directive on the Resilience of Critical Entities (CER) and several other instruments were adopted and also apply to certain financial-sector entities, specifically credit institutions and operators of financial market infrastructures, as well as to providers of digital infrastructure and ICT services who serve the financial sector [i.2] to [i.9].

Responsibility for implementing the DORA, NIS 2 and CER frameworks is assigned to a number of different authorities, both at member-state and Union level. [i.10] In addition, other countries with strong EU bindings have instituted requirements similar to DORA and related harmonisation efforts exist. [Annex B] The present document provides a comprehensive array of related information, including identification of related ETSI Technical Reports and Specifications related to the eight technical standards.

Introduction

As noted by the European Banking Authority [i.11], the European Commission adopted a Digital Finance Package on 24 September 2020, which includes a proposal for a Regulation on "digital operational resilience for the financial sector" (DORA), accompanied by a Directive [i.1]. The overall objective of the DORA legislative package is to make sure the financial sector in Europe is able to effectively manage ICT and cybersecurity risk, including when arising from a third-party provider, and to stay resilient through a severe operational disruption.

The DORA Regulation aims to streamline and upgrade existing rules on:

- ICT Governance and the management of ICT risks (Chapter II);
- the management, classification and reporting of ICT-related incidents (Chapter III);

and to introduce new requirements where gaps exist, particularly with respect to:

- digital operational resilience testing (Chapter IV);
- management of ICT third-party risks and regulation and oversight of 'critical third-party ICT service providers' (CTPPs) (Chapter V);
- information sharing (Chapter VI); and
- the tools the financial supervisors need to fulfil their mandate to contain financial instability stemming from those ICT vulnerabilities (Chapter VII).

The DORA Directive is then tasked with amendments to financial services directives to introduce cross-references to the DORA Regulation and to update empowerments for technical standards. See Annex A.

The first set of final draft technical standards under DORA were released on 17 January 2024 and supplemented throughout the year [i.34]. DORA came into effect on 17 January 2025. There are six major sets of requirements:

- **ICT risk management.** "*Financial institutions must proactively manage risks associated with information and communication technology (ICT)*" (Chapter II, Articles 5 to 16).
- **Handling, classification and reporting of ICT-related incidents.** "*Financial institutions must promptly report significant cyber incidents to relevant authorities*" (Chapter III, Articles 17 to 23).
- **Digital operational resilience testing including threat-led penetration testing (TLPT).** "*Financial institutions must regularly test their ICT systems to identify vulnerabilities and ensure preparedness for cyber threats*" (Chapter IV, Articles 24 to 27).
- **ICT Third-party risk management.** "*Financial institutions must conduct due diligence and ongoing monitoring to ensure third-party compliance with cybersecurity standards*" (Chapter V, Section I, Articles 28 to 30).
- **Oversight of critical third-party providers (CTTP).** "*Service providers whose disruption could significantly impact the financial sector's ability to deliver essential functions based on certain are subject to certain requirements. CTTPs range from data centres and telecommunication providers to software vendors*" (Chapter V, Section II, Articles 31 to 44).
- **Agreements on the exchange of information and cyber crisis and emergency exercises.** "*Financial institutions should share insights, threat intelligence, and best practices with peers*" (Chapter VI Article 45 and Chapter VII Articles 24 to 49).

Virtually all supervised institutions and companies in the European financial sector are covered by DORA. In addition, DORA brings together various requirements for institutions and companies in terms of cybersecurity, ICT risks and digital operational resilience. Entities such as BaFin and the Deutsche Bundesbank are also preparing for DORA - in particular by adapting supervisory and administrative practices and implementing IT processes and systems within the framework of DORA [i.54]. The EC also adopted revised rules for the electronic payment services sector [i.55].

In early 2025, the European Commission requested revision of a number of the Regulatory Technical Standards and suggested amendments. The ESAs have undertaken a process of revising the RTS and ITS standards with a timeline extending through 2025 [i.56].

1 Scope

The present document studies the requirements, available standards, tools, and gaps for implementing the DORA (Regulation (EU) 2022/2554 [i.1]) together with guidance relating to the use of encryption and post-quantum safeguards.

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 (Text with EEA relevance).

[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) (Text with EEA relevance).

[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 (Text with EEA relevance).

[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) (Text with EEA relevance).

[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 (Text with EEA relevance).

[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) (Text with EEA relevance).

[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) (Text with EEA relevance).

[i.9] Resolution (EC) 13084/1/20: "Council Resolution on Encryption - Security through encryption and security despite encryption".

[i.10] ESMA, European Securities and Markets Authority, Securities and Markets Stakeholder Group: "Advice to ESMA, SMSG advice to ESMA on potential practical challenges regarding the implementation of the Digital Operational Resilience Act".

[i.11] European Banking Authority, Banking Stakeholder Group, GSG own initiative paper on DORA.

[i.12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167 /2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance.

[i.13] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).

[i.14] Opinion of the European Economic and Social Committee on 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)'.

[i.15] Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines.

[i.16] ESMA: Consultation on the first batch of Digital Operational Resilience Act (DORA) policy products.

[i.17] ESMA: Consultation Paper, Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA), 5 October 2023.

[i.18] Commission Delegated Regulation (EU) 2024/1505 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by determining the amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid.

[i.19] European Central Bank: "TIBER-EU Framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming".

[i.20] ESMA: "ESMA to put cyber risk as a new Union Strategic Supervisory Priority".

[i.21] ESMA: ESAs joint consultation on second batch of policy mandates under the Digital Operational Resilience Act From 08 December 2023 to 04 March 2024.

[i.22] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.23] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.24] ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".

[i.25] ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.26] ETSI TS 103 523-3: "CYBER; Middlebox Security Protocol; Part 3: Enterprise Transport Security".

[i.27] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.28] ETSI TR 103 619: "CYBER; Migration strategies and recommendations to Quantum Safe schemes".

[i.29] ETSI GR ETI 001: "Encrypted Traffic Integration (ETI); Problem Statement".

[i.30] ETSI GR ETI 006: "Encrypted Traffic Integration (ETI); Implementation of the EU Council Resolution on Encryption".

[i.31] FDIC Banker Resource Center Information Technology (IT) and Cybersecurity.

[i.32] FINA, Cybersecurity.

[i.33] FS-ISAC, Financial Services Information Sharing Analysis Center.

[i.34] EBA, EIOPA, ESMA Final Report JC 2023 83 describes the Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554.

[i.35] EBA, EIOPA, ESMA Final Report JC 2023 84 describes the Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554.

[i.36] EBA, EIOPA, ESMA Final Report JC 2023 85 describes the Draft Regulatory Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/25544.

[i.37] EBA, EIOPA, ESMA Final Report JC 2023 86 describes the Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554.

[i.38] ETSI TR 103 959: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Cloud sector".

[i.39] ETSI TR 103 331: "Cyber Security (CYBER); Structured threat information sharing".

[i.40] ETSI TR 104 034: "Cyber Security (CYBER); Software Bill of Materials (SBOM) Compendium".

[i.41] ESMA: ESAs joint consultation on second batch of policy mandates under the Digital Operational Resilience Act.

[i.42] EBA: Consultation on Joint draft RTS specifying elements related to threat led penetration tests.

[i.43] FS-ISAC: Preparing for a Post-Quantum World by Managing Cryptographic Risk, March 2023.

[i.44] Cloud Security Alliance: "The State of Cyber Resiliency in Financial Services".

[i.45] EBA: "ESAs published second batch of policy products under DORA".

[i.46] C(2024) 6901 final: Commission Delegated Regulation (EU) …/... of 23.10.2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT related incidents, and the content of the voluntary notification for significant cyber threats (Text with EEA relevance).

[i.47] C(2024) 7277 final: Commission Implementing Regulation (EU) …/... of 23.10.2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat (Text with EEA relevance).

[i.48] C(2024) 6913 final: Commission Delegated Regulation (EU) …/... of 24.10.2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards on harmonisation of conditions enabling the conduct of the oversight activities (Text with EEA relevance).

[i.49] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance.

[i.50] EN 18031-3: "Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value" (produced by CEN).

[i.51] Payment Card Industry: Data Security Standard, Requirements and Testing Procedures.

[i.52] EBA, EIOPA, ESMA: Report on the feasibility for further centralisation of reporting of major ICT-related incidents.

[i.53] EBA: The EBA repeals the Guidelines on major incident reporting under the revised Payment Services Directive.

[i.54] Federal Financial Supervisory Authority (BaFin): DORA - Digital Operational Resilience Act.

[i.55] European Commission: Payment services: revised rules to improve consumer protection and competition in electronic payments.

[i.56] Cyber Risk GmbH: DORA | Updates, Compliance.

[i.57] ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.58] ETSI TR 103 990: "Cyber Security (CYBER); Standards mapping and gap analysis against regulatory expectations".

[i.59] ETSI TS 103 963: "CYBER; Optical Network and Device Security; Security provisions in transport network devices".

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:

AI	Artificial Intelligence
CER	Critical Entities Resilience
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EC	European Commission
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ESA	European Supervisory Agency
ESMA	European Securities and Markets Authority
EU	European Union
EuID	European unique Identifier
FDIC	Federal Deposit Insurance Corporation
ICT	Information and Communication Technology
IT	Information Technology
ITS	Implementing Technical Standard
NIS2	Network and Information Security directive 2
PCI DSS	Payment Card Industry Data Security Standard

RED	Radio Equipment Directive
RTS	Regulatory Technical Standard(s)
SBOM	Software Bill Of Materials
TPP	Third-Party Provider
VLOP	Very Large Online Platform

4 DORA Implementation

4.0 Introduction

In June 2023, ESMA released a set of Consultation Papers establishing the requirements and related standards. The consultation period ran to 11 September 2023 [i.16]. The consultation was finalized in 17 January 2024 with the release of four standards-related reports discussed in clause 4.1 below, [i.34] to [i.37].

4.1 Standards Requirements

4.1.0 Organization and description of the requirements

The chapters are clustered into six groups described below that primarily describe the financial authority standards developed pursuant to DORA. The considerable complexity of these requirements combined with variants for specific financial sectors, other EU legislative instrument implementations and the transpositions into EU Member State versions pose a significant continuing challenge to fully articulating the applicable standards.

In early 2025, the European Commission rejected a number of the Regulatory Technical Standards and suggested amendments. The ESAs have undertaken a process of revising the RSAs with a timeline extending through 2025 [i.56].

4.1.1 Proportionality

DORA Article 4 requires that financial entities implement rules in accordance with the principal of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations as applied to the subsequent chapters of the Act [i.1].

4.1.2 ICT risk management

Chapters I and II of DORA contain DORA Articles 5 to 16 that treat risk management in financial institutions:

- Article 5, Governance and organization
- Article 6, ICT risk management framework
- Article 7, ICT systems, protocols and tools
- Article 8, Identification
- Article 9, Protection and prevention
- Article 10, Detection
- Article 11, Response and recovery
- Article 12, Backup policies and procedures, restoration and recovery procedures and methods
- Article 13, Learning and evolving
- Article 14, Communication
- Article 15, Further harmonisation of ICT risk management tools, methods, processes and policies

- Article 16, Simplified ICT risk management framework

Standards were developed by the financial authorities pursuant to Articles 10, 15, and 16 that address most if not all of the risk management requirements.

Article 10, Harmonisation of reporting content and templates

Harmonisation of reporting content and templates occurred through "dry run" for the templates and tools announced in April 2024 and based on the Implementing Technical Standards published in January 2024 to the Commission and published by the Commission in late 2024 [i.41].

Article 15, Further harmonisation of ICT risk management tools, methods, processes and policies

ESMA consultation paper JC 2023 39 describes the draft Regulatory Technical Standards (RTS) to further harmonise ICT risk management tools, methods, processes and policies for Article15 [i.16].

EBA, EIOPA, ESMA Final Report JC 2023 86 [i.37] describes the Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554 [i.1].

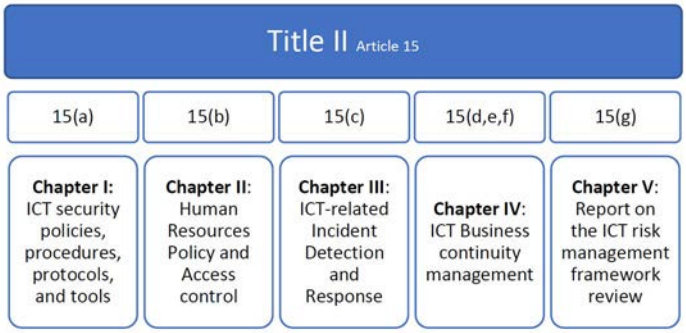

Figure 4.1-1: Regulatory Technical Standards (RTS) mandated under Article 15 [i.37]

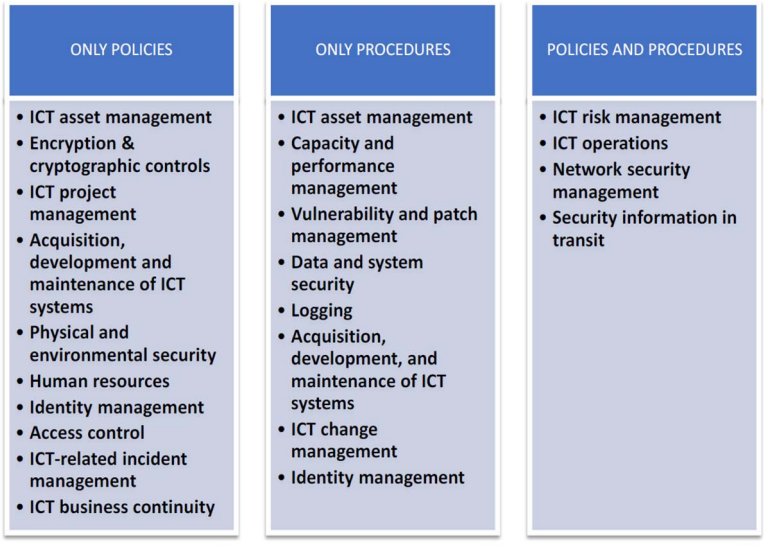

Figure 4.1-2: Overview of the policies and procedures required under Article 15 [i.37]

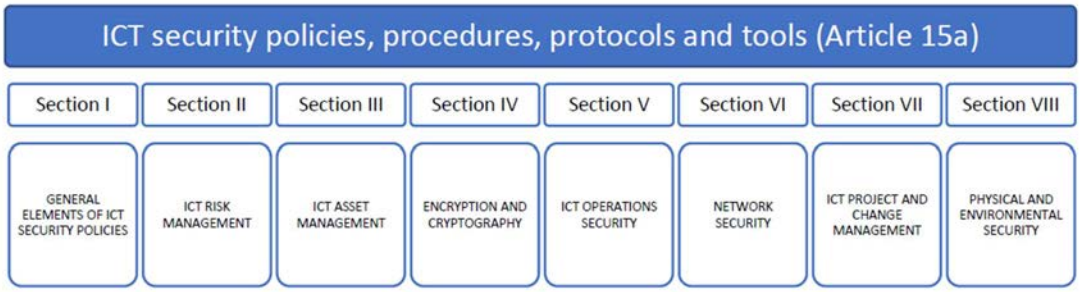

Figure 4.1-3: Mapping of Regulatory Technical Standards for DORA risk management [i.37]

The provisions of the DORA ICT Risk Management Framework is similar to ETSI CYBER Critical Security Controls and the Cloud Sector and NIS2 implementation guidelines [i.22] to [i.26] and [i.38].

Article 16, Simplified ICT risk management framework

ESMA consultation paper JC 2023 39 describes the draft regulatory technical standards to further harmonise ICT risk management tools, methods, processes and policies for Article16(3) [i.16].

EBA, EIOPA, ESMA Final Report JC 2023 86 [i.37] describes the Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554.

As noted in the Report "*in general, the approach followed by the ESAs in identifying the requirements for the financial entities that are subject to the simplified ICT risk management framework, was to focus on those essential areas and elements that are at a minimum necessary to ensure the confidentiality, integrity, availability and authenticity of their data and services, while considering their scale, risk, size and complexity. In this context, these financial entities should have in place an internal governance and control framework with clear responsibilities to enable an effective and sound risk management framework*" [i.37]. The simplified framework is depicted in Figure 4.1-4 below.

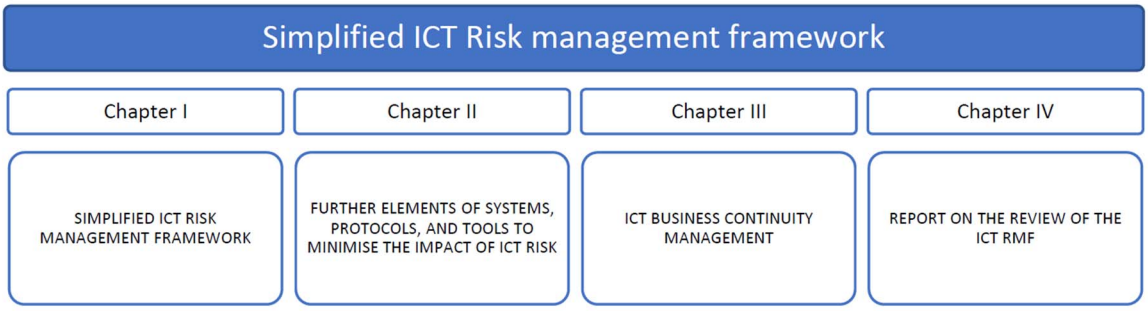

Figure 4.1-4: Simplified DORA risk management framework [i.37]

The framework roughly corresponds to Critical Security Controls Implementation Group 1 [i.22].

4.1.3 Handling, classification and reporting of ICT-related incidents

Chapter III of DORA contains Articles 17 to 23 treating handling, classification and reporting of ICT-related incident:

- Article 17, ICT-related incident management process
- Article 18, Classification of ICT-related incidents and cyber threats
- Article 19, Reporting of major ICT-related incidents and voluntary notification of significant cyber threats
- Article 20, Harmonisation of reporting content and templates
- Article 21, Centralization of reporting of major ICT-related incidents
- Article 22, Supervisory feedback

- Article 23, Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions

Standards were developed by the financial authorities pursuant to Articles 18 and 21 that address Chapter III requirements.

Article 18, Classification of ICT-related incidents and cyber threats

ESMA consultation paper JC 2023 34 describes the draft regulatory technical standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats for Article 18 [i.16].

EBA, EIOPA, ESMA Final Report JC 2023 83 [i.34] describes the Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554.

The published classification criteria trigger DORA reporting requirements. See Figure 4.1-5 below.

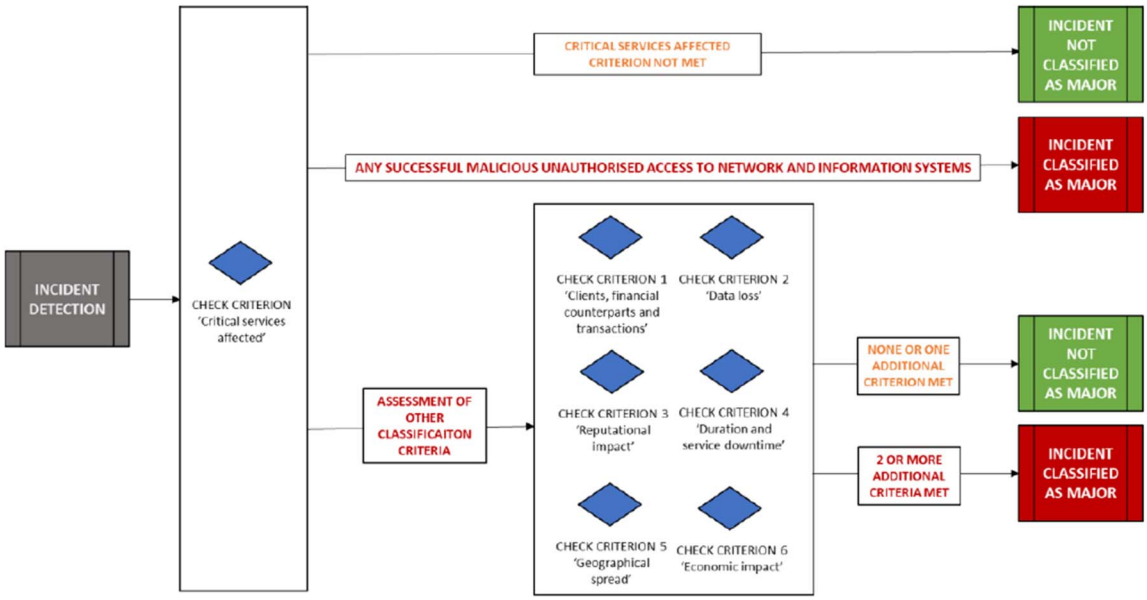

Figure 4.1-5: Approach for classifying major incidents under DORA [i.34]

In general, ETSI's standards publications relating to structured threat information sharing and NIS2 implementation can support an array of major incident information sharing [i.39] and [i.25].

Article 21, Centralization of reporting of major ICT-related incidents

The ESAs, through the Joint Committee, and in consultation with the ECB and ENISA, were required to prepare a joint report assessing the feasibility of further centralization of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities [i.52]. The joint report explores ways to facilitate the flow of ICT-related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence. As of 17 January 2025, the new guidelines apply. DORA introduced harmonised incident reporting requirements that apply to financial entities across the banking, securities/markets, insurance, and pensions sectors, including most payment service providers [i.53].

4.1.4 Digital operational resilience testing including Threat-Led Penetration Testing (TLPT)

Chapter IV of DORA contains Articles 24 to 27 treating operational resilience testing:

- Article 24, ICT-related incident management process
- Article 25, Classification of ICT-related incidents and cyber threats

- Article 26, Reporting of major ICT-related incidents and voluntary notification of significant cyber threats
- Article 27, Harmonisation of reporting content and templates

Standards were developed pursuant to Article 26 that address Chapter IV requirements.

Article 26, Advanced testing of ICT tools, systems and processes based on threat-led penetration testing

Responses to the public consultations on the Consultation paper on Joint draft RTS specifying elements related to threat led penetrations tests were submitted in March 2024 and awaiting further action by the EBA [i.42]. The TLPT participants are depicted in Figure 4.1-6.

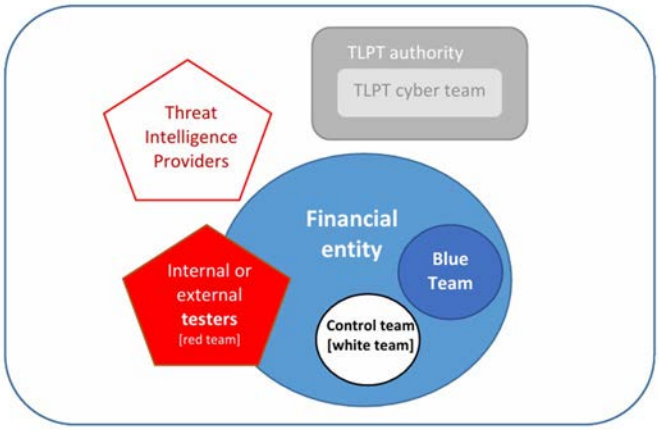

Figure 4.1-6: Structure of the Register of Information under DORA [i.42]

4.1.5 ICT third-party risk management

Chapter V Section I of DORA contains Articles 28 to 30 treating ICT third-party risk management:

- Article 28, General principles
- Article 29, Preliminary assessment of ICT concentration risk at entity level
- Article 30, Key contractual provisions

Standards were developed by the financial authorities pursuant to Articles 28 and 30 that address Chapter V Section I requirements.

Article 28, General Principles for a sound management of ICT third-party risk

ESMA consultation paper JC 2023 36 describes the draft regulatory technical standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers for Article 28.9 [i.16].

ESMA consultation paper JC 2023 35 describes the draft regulatory technical to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers for Article 28.10 [i.16].

EBA, EIOPA, ESMA Final Report JC 2023 84 [i.35] describes the Draft Regulatory Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/25544 [i.36]. The financial entity's policy on the use of ICT third-party service providers is defining crucial parts of the financial entities' governance arrangements, risk management and internal control framework with regard to the use of ICT services provided by ICT third-party service providers and should ensure that the financial entity remains in control of its operational risks, information security and business continuity throughout the life cycle of contractual arrangements with such providers.

The Commission Delegated Regulation adopted as part of the Final Report sets forth ten provisions for specifying the detailed policy and contractional arrangements for ICT services supporting critical or important functions provided by ICT third-party providers [i.35]:

- Article 1, Overall risk profile and complexity
- Article 2, Group application
- Article 3, Governance arrangements regarding the policy on the use of ICT services supporting critical or important functions
- Article 4, Main phases of the life cycle for the use of ICT services supporting critical or important functions provided by ICT third- party service providers
- Article 5, Ex-ante risk assessment
- Article 6, Due diligence
- Article 7, Conflict of interests
- Article 8, Contractual clauses for the use of ICT services supporting critical or important functions
- Article 9, Monitoring of the contractual arrangements for the use of ICT services supporting critical or important functions
- Article 10, Exit and termination of contractual arrangements for the use of ICT services supporting critical or important functions

Article 30, Key contractual provisions

EBA, EIOPA, ESMA Final Report JC 2023 85 [i.36] describes the Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554. The provisions include provisions relating to the structure of the Registration of information and the outsourcing process as shown in Figures 4.1-7 and 4.1-8 below.

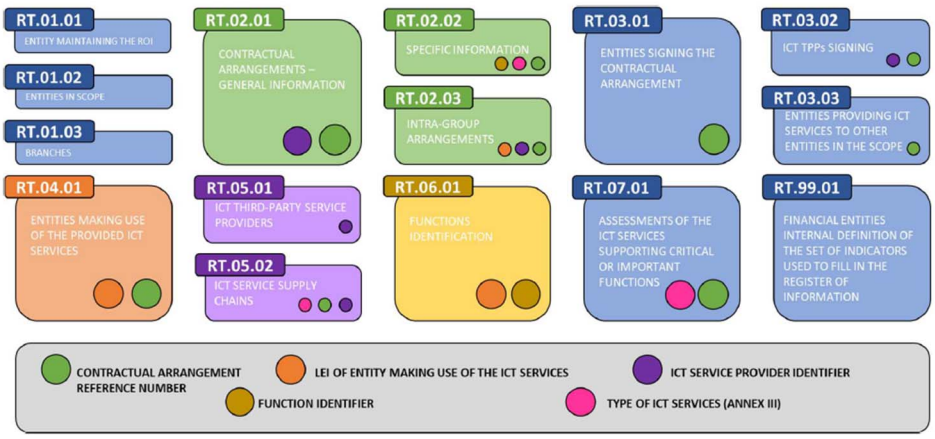

Figure 4.1-7: Structure of the Register of Information under DORA [i.36]

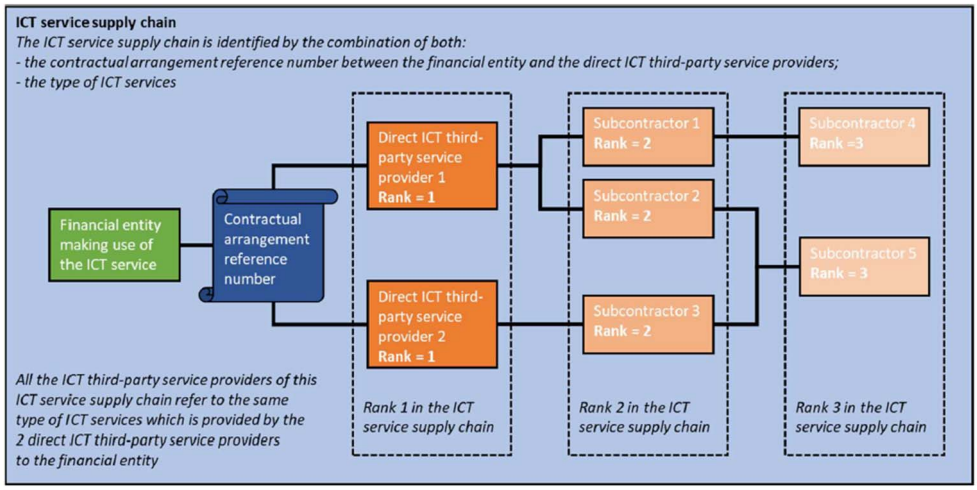

Figure 4.1-8: ICT service supply chain example under DORA [i.36]

These DORA requirements have a nexus to nexus to ETSI SBOM supply chain standards activities [i.40].

4.1.6 Oversight of critical third-party providers (CTTP)

Chapter V Section II of DORA contains Articles 31 to 44 treating oversight of critical third-party providers:

- Article 31, Designation of critical ICT third-party service providers
- Article 32, Structure of the Oversight Framework
- Article 33, Tasks of the Lead Overseer
- Article 34, Operational coordination between Lead Overseers
- Article 35, Powers of the Lead Overseer
- Article 36, Exercise of the powers of the Lead Overseer outside the Union
- Article 37, Request for information
- Article 38, General investigations
- Article 39, Inspections
- Article 40, Ongoing oversight
- Article 41, Harmonisation of conditions enabling the conduct of the oversight activities
- Article 42, Follow-up by competent authorities
- Article 43, Oversight fees
- Article 44, International cooperation

Standards were developed by the financial authorities pursuant to Article 41 that address Chapter V Section II requirements.

Article 41, Harmonisation of conditions enabling the conduct of the oversight activities

The Consultation Paper on draft Guidelines on oversight cooperation was published and comments received [i.41].

4.1.7 Agreements on the exchange of information and cyber crisis and emergency exercises

Chapter VI Article 45 and Chapter VII Articles 46 to 49 treating agreements on the exchange of information and cyber crisis and emergency exercises:

- Article 45, Information-sharing arrangements on cyber threat information and intelligence
- Article 46, Competent authorities
- Article 47, Cooperation with structures and authorities established by Directive (EU) 2022/2555 [i.2]
- Article 48, Cooperation between authorities
- Article 49, Financial cross-sector exercises, communication and cooperation

No standards were developed by the financial authorities that address Chapters VI and VII requirements.

4.2 Available standards and tools

In general, the Critical Security Controls, facilitation mechanisms, and various implementation guides - especially for Cloud Computing and NIS2 provide significant available standards and tools [i.22] to [i.26] and [i.38].

ETSI TC ESI in ETSI EN 319 401 [i.57] for Trust Service Provider incident response policy requirements added REQ-7.9.2-02X for DORA compliance. TC CYBER added a reference to potential DORA compliance requirements for optical network and device security ETSI TS 103 963 [i.59] as well as a note in the standards mapping against regulatory explanations ETSI TR 103 990 [i.58].

The Payment Card Industry Data Security Standard (PCI DSS) [i.51] may also apply and help meet DORA risk management standards. The ETSI Critical Security Controls has a mapping to the PCI DSS.

4.3 Avoiding duplication

4.3.1 Problem statement

As the EBA notes [i.11], two other legislative acts of relevance, the CER Directive and the NIS 2 Directive have been adopted. The banking sector has been designated as a "sector of high criticality" for the purposes of the NIS 2 and CER Directives and credit institutions are liable to be designated as "essential" or "important entities" under NIS 2. While DORA qualifies as a "sector-specific Union act" (*lex specialis*) and financial institutions that are within its scope are therefore exempted from certain obligations laid down in NIS 2 (recital 13 and Article 2) these entities will still be bound by both frameworks and subject to the supervision of the respective competent authorities tasked with their implementation at the national and EU level. This means that potential overlaps still exist and will need to be addressed to avoid duplication. Some overlaps are being treated by the EC using implementing technical regulations. See clause 4.6 below.

The Radio Equipment Directive (RED) [i.49] which sets standards concerning internet-connected radio equipment placed on the market, has an Article 3 3.(f) provision requiring implementation of capabilities for protection against fraud when processing virtual money or anything of monetary value that are addressed in EN 18031-3 [i.50].

4.3.2 EBA recommendations

The European Banking Authority recommended ten actions to avoid unnecessary duplication among the applicable Directives [i.11]:

- Co-ordination between authorities and efficiency
- A coherent regulatory and supervisory approach to operational resilience
- Capacity building and best use of resources

- ICT risk management and internal governance
- The oversight framework of critical ICT Third Party Providers (TPPs)
- The need for developing international standards - incident reporting
- Attaining an adequate level of stakeholder dialogue and collaboration
- Building detailed risk taxonomies
- Testing: adoption and evolution of the TIBER EU framework
- Impact on consumers

4.4 Gaps

A definitive mapping between the DORA requirements and the Critical Security Controls appears to be a useful step as the requirements have reached maturity through the consultative proceedings of the European Banking Authorities as highlighted by the Cloud Security Alliance [i.44].

With the subsequent enactment of the AI Act [i.12], [i.14] and the proposed companion AI Liability Directive [i.13], Financial Service providers subject to DORA risk management requirements will also ensure they are compliant with the requirements of that legislation and considerable commercial tools have become available for those purposes. Similarly, EU risk management related requirements under the AI Act and other legislation requiring the use of SBOMs for products and services may also apply.

Additionally, where some Very Large Online Platforms (VLOPs) also offer financial services, they fall under additional requirements of the Digital Services Act [i.15].

4.5 Post-quantum safeguards

The Financial Services ISAC roadmap for post-quantum preparation consists of set of pre-emptive safeguards [i.43].

4.6 European Commission implementing technical regulations

On 23 and 24 October 2024, the European Commission adopted the following Regulatory Technical Standards (RTS) and Implementing Technical Standard (ITS) through Delegated Regulations supplementing DORA:

- A RTS specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats [i.46].
- An ITS and annex for standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat [i.47].
- A RTS on harmonisation of conditions enabling the conduct of the oversight activities [i.48].

The European Commission has yet to adopt two more RTSs: one on the criteria for determining the composition of the joint examination team and one on threat-lead penetration testing. One more ITS has yet to be adopted because the EC rejected the ITS on the register of information, proposing to include the European Unique Identifier (EuID). The Commission argued that financial entities should have the choice between the EuID and the LEI code when identifying their ICT third-party service providers registered in the EU.

Annex A:
DORA Provisions

A.1 Key Objectives

- Uniform requirements for the security of network and information systems supporting the business processes of financial entities to achieve a high common level of digital operational resilience:
  - Information and Communication Technology (ICT) risk management;
  - reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;
  - reporting of major operational or security payment-related incidents to the competent authorities by credit, payment, and electronic money institutions, and account information service providers;
  - digital operational resilience testing;
  - information and intelligence sharing in relation to cyber threats and vulnerabilities;
  - measures for the sound management of ICT third-party risk;
- Contractual arrangement requirements between ICT third-party service providers and financial entities.
- Establishment and conduct of the Oversight Framework for critical ICT third-party service providers when providing services to financial entities.
- Cooperation among competent authorities, and rules on supervision and enforcement by competent authorities of DORA.
- A sector-specific implementation of the NIS2 Directive.

A.2 Parties subject to DORA

- ICT third-party service providers
- Account information service providers
- Administrators of critical benchmarks
- Central counterparties
- Central securities depositories
- Credit institutions
- Credit rating agencies
- Crowdfunding service providers
- Crypto-asset service providers and issuers of asset-referenced tokens
- Data reporting service providers
- Electronic money institutions
- Institutions for occupational retirement provision
- Insurance and reinsurance undertakings

- Insurance intermediaries, reinsurance intermediaries & ancillary insurance intermediaries
- Investment firms
- Management companies
- Managers of alternative investment funds
- Payment institutions
- Securitisation repositories
- Trade repositories
- Trading venues

A.3 DORA treatment of standards

- Article 5 (Governance and organization) calls for the financial entity management body to put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data.
- Article 9 (Protection and prevention) requires "financial entities design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit".
- Article 15 (Further harmonisation of ICT risk management tools, methods, processes and policies):
  - *The ESAs shall, through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standards.*
  - *When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, while duly taking into consideration any specific feature arising from the distinct nature of activities across different financial services sectors.*
  - *The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.*
- Article 16 (Simplified ICT risk management framework):
  - *The ESAs shall, through the Joint Committee, in consultation with the ENISA, develop common draft regulatory technical standards.*
  - *The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.*
- Article 18 (Classification of ICT-related incidents and cyber threats)
  - *The ESAs shall, through the Joint Committee and in consultation with the ECB and ENISA, develop common draft regulatory technical standard.*
  - *The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.*
- Article 20 (Harmonisation of reporting content and templates):
  - *The ESAs, through the Joint Committee, and in consultation with ENISA and the ECB, shall develop: (a) common draft regulatory technical standards…*
  - *The ESAs shall submit the common draft regulatory technical standards by 17 July 2024.*

- Article 26 (Advanced testing of ICT tools, systems and processes based on TLPT [threat-led penetration testing):
  - *The ESAs shall, in agreement with the ECB, develop joint draft regulatory technical standards.*
  - *The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.*
- Article 28 (General Principles [for a sound management of ICT third-party risk]}:
  - *The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the register of information…, including information that is common to all contractual arrangements on the use of ICT services. The ESAs shall submit those draft implementing technical standards to the Commission by 17 January 2024.*
  - *The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to further specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.*
  - *When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.*
- Article 30 (Key contractual provisions):
  - *The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements…which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.*
  - *When developing those draft regulatory technical standards, the ESAs shall take into consideration the size and overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations.*
  - *The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.*
- Article 33 (Tasks of the Lead Overseer):
  - *…assessment…shall cover…the use of relevant national and international standards applicable to the provision of its ICT services to the financial entities.*
- Article 41 (Harmonisation of conditions enabling the conduct of the oversight activities):
  - *The ESAs shall, through the Joint Committee, develop draft regulatory technical standards.*
  - *The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.*

A.4 DORA regulatory standards deliverables

17 January 2024, Article 15 Further harmonisation of ICT risk management tools, methods, processes and policies:

- Article 16 Simplified ICT risk management framework
- Article 18 Classification of ICT-related incidents and cyber threat
- Article 28 General Principles for a sound management of ICT third-party risk

17 July 2024, Article 10 Harmonisation of reporting content and templates:

- Article 26 Advanced testing of ICT tools, systems and processes based on threat-led penetration testing
- Article 30 Key contractual provisions
- Article 41 Harmonisation of conditions enabling the conduct of the oversight activities

A.5 DORA treatment of encryption

- Article 9 4 requires financial entities:
  - 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.
- Article 35 1(d)(i) empowers the Lead Overseer to "issue recommendations concerning:
  - the use of specific ICT security and quality requirements or processes, in particular in relation to the roll-out of patches, updates, encryption and other security measures which the Lead Overseer deems relevant for ensuring the ICT security of services provided to financial entities.
- *Council Resolution on Encryption* adopted on 14 December 2020 notes that certain types of end-to-end encryption pose fundamental challenges:
  - For Member States protecting essential security interests.
  - For network service providers in meeting an array of compliance obligations, including cybersecurity risk management.
  - Calls for cooperation on solutions for meeting these requirements.

Annex B:
Non-EU Cybersecurity Regulations for Financial Services

B.1 FS-ISAC Financial Services Information Sharing and Analysis Center

The FS-ISAC site provides a portal to the global cyber intelligence sharing community focused on financial services among institutions in more than 70 countries. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyber threats [i.33].

B.2 United States Cybersecurity Regulations for the Sector

B.2.1 FDIC Banker Resource Center for Cybersecurity

The FDIC Banker Resource Center provides a broad structured enumeration of resources on its Information Technology (IT) and Cybersecurity site [i.31]. The resources include:

- Laws and Regulations
- Supervisory Resources:
  - Cybersecurity
  - IT Security
  - Authentication
  - Identity Theft
  - Third-Party Relationships
  - Payments
  - Business Continuity Management
- Other Resources:
  - FFIEC Industry Outreach Website provides resource materials on current issues in the financial industry, including Information Technology and Cybersecurity.
  - FFIEC Cybersecurity Awareness Website provides resources to increase awareness of cybersecurity risks and to assess and mitigate cybersecurity risks.
  - NIST Cybersecurity Framework Website provides information on a voluntary cybersecurity framework developed by the National Institute of Standards and Technology.
  - Technology Outsourcing: Informational Tools for Community Bankers provides resources for selecting service providers, drafting contract terms, and providing oversight for multiple service providers.

B.2.2 FINRA Cybersecurity

The FINRA Rules & Guidance resource site provides a broad structured enumeration of cybersecurity resources and guidance on its site, including advisory and vulnerability alerts [i.32].

B.3 Swiss Financial Sector Cyber Security Centre

The Swiss FS-CSC association provides for the operation of its Operational Cyber Security Cell (OCS) through FS-ISAC (Financial Services Information Sharing and Analysis Centre), and provides Swiss banks and insurance companies with cyber security, including threat reporting and assessments, planning and implementation of measures in crisis situations, as well as exercises and support in the event of cyber attacks.

Annex C: Bibliography

- Carnegie Endowment for International Peace: "The European Union, Cybersecurity, and the Financial Sector: A Primer", 16 March 2021.
- Central Bank of Ireland: "Implementing DORA - Achieving enhanced digital operational resilience in European financial services".
- Ernst & Young: "How to prepare for the Digital Operational Resilience Act?".
- Google®: "DORA's implementation period starts now. What we're doing to prepare for the new law".
- IBM®: "The Digital Operational Resilience Act for Financial Services: Harmonised rules, broader scope of application".
- Lexology: "All you need to know about DORA: New obligations for the financial sector".
- SecurityIntelligence: "DORA and your quantum-safe cryptography migration".
- IT Security News: "DORA and your quantum-safe cryptography migration".
- SBOM Observer Academy: "DORA - Digital Operational Resilience Act".

History

Document history		
V1.1.1	May 2025	Publication