DORA in Control

A Practical Guide to Achieve Enhanced Digital Operational Resilience

A study report by NOREA

Authors:

S. Gangaram Panday – Schuberg Philis

J. Oschmann – Schuberg Philis

PO box 242, 2130 AE Hoofddorp

Phone: +31 (0) 88 4960 380

The Netherlands

e-mail: norea@norea.nl

Taskforce participants

The study report and framework were reviewed by the following members of the NOREA DORA Taskforce:

Name	Role	Company
Harry Boersen	Director Tech Advisory	Yaworks
Danny Bos	Senior manager Cybersecurity & Privacy	Eraneos
Ibrahim Dogan	Register IT-Auditor	Validacy
Otto Hulst	Beleidsadviseur	Pensioenfederatie
Arno Kroese	Director IT Assurance & Advisory	KPMG
Marvin Kruin	Register IT-Auditor	MNK Risk, Audit & Advisory Services
René Zendijk	Head of Internal Audit	Scildon
Shairesh Algoe	CISO Manager IT Security	Quantum Gateway Foundation BNG Bank

For the full member list and more content created by the Taskforce, please see https://www.norea.nl/dora

Endorsements of the study report and framework

This study report and the control framework presented in this paper are endorsed by the following financial industry associations:

nederlandse vereniging van banken · VERBOND VAN VERZEKERAARS · PENSIOEN FEDERATIE · VBIN Verenigde Betaal Instellingen Nederland

The study report and Dora in control framework have been shared with the DNB and AFM. The supervisory authorities provided the following joint response:

"DNB and AFM took note of the framework prepared by NOREA to provide guidance to the industry on practical implementation of DORA. DNB and AFM did not contribute to its development. Nor has the framework been assessed by DNB and AFM in terms of content. However, the development of such frameworks is in line with previous calls from DNB and AFM to work together within the sector to increase the overall cyber resilience of the sector and, if desired, to mutually develop and update standards that can contribute to this. DNB and AFM stress that complying with applicable laws and regulations is at all times a responsibility of the institution. No confidence can be derived from the use of such a framework that parties thereby act in line with laws and regulations."

The DORA in control framework presented in this study report was developed in collaboration with Schuberg Philis.

Table of contents

1 Introduction

1.1 Motivation

A rapidly evolving landscape of digital threats has hastened the already urgent need for organizations to have robust, adaptable frameworks that ensure operational resilience. Financial institutions, in particular, are facing unprecedented challenges not only from cyberthreats, but also from the complex regulatory environment designed to safeguard their operations.

One such regulation, the Digital Operational Resilience Act (DORA), introduced by the European Union (EU), is a landmark initiative aimed at enhancing the digital operational resilience of the financial sector. However, the more DORA stakeholders we engage with, the more it has become clear that the act's requirements sometimes present significant interpretation challenges for financial institutions.

We were motivated to develop the DORA in control framework upon witnessing the difficulties that financial institutions face in translating the act's regulations into practical, actionable measures. Adding to the complexity is the financial sector's growing reliance on digital systems, compounded by the increasingly interconnected nature of global finance. As a result, a relatively small operational disruption can have far-reaching consequences. Moreover, the importance of compliance is heightened by the potential societal impact of digital failures, which can extend beyond individual institutions to disrupt services essential to the public.

At the time of writing, no comprehensive framework exists to guide financial institutions in effectively navigating DORA's requirements. While DORA is a monumental step toward safeguarding the financial sector and it does give detailed requirements, the act is composed in a way that leaves room for interpretation. With this in mind, we set out to construct a framework that simplifies all the legal and technical complexities. Our goal was to turn DORA's regulatory requirements into practical, actionable measures that financial institutions can understand and implement.

For readers interested in the broader context of DORA and digital resilience, the full report provides valuable background. For those eager to begin the implementation process, focusing on Chapter 4 and the consolidated controls therein presents a clear path forward.

We envision the DORA in control framework as a living tool, capable of evolving in response to both regulatory changes and emerging digital risks. Working together to ensure that digital operational resilience is not only a regulatory requirement but a cornerstone of sustainable financial operations in a digital world, we encourage feedback and engagement from stakeholders across the financial sector.

From the authors,

Sandeep Gangaram Panday - sgangarampanday@schubergphilis.com

Jeremy Oschmann – joschmann@schubergphilis.com

1.2 Executive summary

The Digital Operational Resilience Act (DORA) came into force on 16 January 2023 and will apply as of 17 January 2025. Once DORA applies, organizations operating or providing services for the financial sector will be expected to have undergone significant changes and be prepared to abide by new requirements. Recognizing the complexity and challenges associated with interpreting and implementing such provisions, we developed a practical framework designed to assist institutions in navigating these new regulatory waters.

We are proud to introduce the DORA in control framework, a tool that translates complex legal texts into actionable, consolidated controls and, as such, helps financial institutions achieve digital resilience. Our framework is built around three key objectives to enable successful implementation:

1. To simplify and translate DORA so a broader audience can understand its contents and the rationale behind the regulations.
2. To assist organizations in running DORA gap assessments and preparing related reports for supervisory authorities.
3. To examine DORA from an engineering perspective, aiming to solve actual root causes of issues in their information and communication technology (ICT) environment and to help businesses achieve sustainable operational resilience.

In addition, the DORA in control framework may be of use to organizations falling within the scope of the EU's Network and Information Security Directive 2 (NIS2). DORA and NIS2 share the same ambition: to enhance cybersecurity and operational resilience. Because NIS2 merely outlines high-level goals, however, affected organizations have been uncertain about what to do and how to implement it. In contrast, DORA offers specific, detailed rules, many of which are stringent and align with the core principles of the Duty of Care outlined in NIS2. Therefore, we recommend that organizations subject to NIS2 regulations use the DORA control framework as a resource to help achieve compliance with NIS2.

The full excel version of the DORA in control framework is available on the NOREA website at https://www.norea.nl/dora

We encourage you to refer to the framework, download the file, and contribute to keeping the information relevant and rigorous by sharing your comments and feedback with the authors.

2 Background on DORA

2.1 From security to resilience

In recent years, the focus of information and communication technology (ICT) within the financial sector has shifted from cybersecurity toward comprehensive resilience. This transition reflects the evolving landscape of threats and dependencies in an increasingly digital and interconnected market. Historically, the primary concern for financial institutions had been securing ICT systems against unauthorized access, data breaches, and cyberattacks. This security-specific approach, while necessary, often fell short of addressing the full spectrum of risks that could disrupt business operations.

The digital transformation of the financial industry combined with growing threats from criminals and state actors has heightened the level and complexity of threats overall. Accordingly, today's resilience strategies must not only address cyberthreats, but also encompass operational continuity measures across all ICT services critical to financial stability. After all, financial institutions now rely heavily on ICT systems not just for transaction processing, but for a myriad of critical business functions, including trading, fraud detection, and treasury management.

Such dependency on ICT systems means that any failure, whether due to a cyberattacks, technical malfunction, or another unforeseen event, can have far-reaching consequences. Disruptions can affect the availability, authenticity, integrity, and confidentiality of financial services, leading to financial losses, reputational damage, and erosion of customer trust. As these systems have become integral to the day-to-day operations of financial entities, the potential impact of their disruption has grown exponentially toward an extinction-level threat for institutions. Moreover, the interconnectedness of the global financial system means that a failure in one entity can have cascading effects, potentially leading to systemic risks with vast and varied socioeconomic effects.

This shift aligns with a new focus on ensuring the integrity and availability of services under all conditions, thereby mitigating the risk of systemic disruptions in the financial sector. In the context of legislation, resilience refers to the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.[1]Such a holistic approach to resilience can encompass a range of strategies, from cyber defense and ransomware incident response plans to business operations recoverability strategies, actual recovery testing, and advanced crisis management.

2.2 European digital strategy

The EU unequivocally recognizes the need to promote digital resilience within its broader digital strategy.[2] New legal acts and regulatory frameworks have been introduced to enhance digital resilience and harmonization across the financial sector. These measures aim to create a robust regulatory environment that not only enhances the security of ICT systems, but also fortifies the resilience of critical business functions that depend on them. Examples of legal acts within the EU digital strategy are:

- Digital Operational Resilience Act (DORA)
- Network and Information Security 2 (NIS2) Directive
- Critical Entities Resilience (CER) Directive
- Cyber Resilience Act (CRA)
- Cybersecurity Act

[1] https://csrc.nist.gov/glossary/term/cyber_resiliency
[2] https://eufordigital.eu/discover-eu/eu-digital-strategy/

- Cyber Solidarity Act

These new regulations mandate that critical entities (entailing their complete ecosystem) establish and maintain comprehensive resilience strategies, including regular testing, risk management, and governance protocols. In doing so, the regulations enable the organizations to sustain operations and protect stakeholders even in the face of significant disruptions.

The emphasis on resilience acknowledges that in a digital age, the question is not if disruptions will occur, but when. Thus, financial institutions must be prepared to manage and mitigate the impact of such events. Building resilience into ICT systems and business processes ensures continuity, stability, and confidence in the financial market, all of which are essential for economic health and public trust.

2.3 Regulating digital operational resilience

In light of the evolving and increasing dependencies on ICT systems, the EU introduced DORA to address multifaceted risks within the financial sector. DORA marks a significant shift in the EU's broader regulatory framework. Now emphasized is the importance of digital operational resilience to safeguard the stability and integrity of the financial market.

Officially known as Regulation (EU) 2022/2554, DORA is a legislative act intended to ensure that financial entities within the EU can withstand, respond to, and recover from all types of ICT-related disruptions and threats. It consolidates and enhances existing ICT requirements, constructing a unified framework for digital operational resilience across the European financial sector.

Despite previous regulatory efforts undertaken at both national and EU-wide levels, significant gaps and inconsistencies in addressing ICT risks have prevailed. The European Systemic Risk Board highlighted in a 2020 report[3] the systemic vulnerability posed by the high level of interconnectedness and interdependencies within the financial sector's ICT systems. These vulnerabilities necessitated a more comprehensive and harmonized approach to ICT risk management, precisely which DORA aims to provide.

2.3.1 What DORA aims to achieve

DORA specifies numerous requirements to help organizations build and maintain digital operational resilience. These requirements are centered around five pillars:

1. ICT risk management
2. Incident management, classification, and reporting
3. Digital operational resilience testing
4. Managing of ICT third-party risks
5. Information-sharing arrangements

2.3.2 How DORA aims to achieve its objectives

DORA lays out several key requirements, referred to as level 1 regulations, to achieve its objectives. Described in the act itself, these requirements are discussed in the context of DORA's five foundational pillars.

1) ICT risk management – DORA chapter 2 (articles 5 – 16):

[3] European Systemic Risk Board, Annual Report 2020, https://www.esrb.europa.eu/pub/pdf/ar/2021/esrb.ar2020~f20842b253.en.pdf

ICT risk management requires financial entities to establish comprehensive frameworks to identify, protect against, detect, respond to, and recover from ICT-related risks. This first pillar pushes for clear governance, regular risk assessments, protective measures, detection systems, incident response plans, and continuous improvement based on past experiences.

2) ICT-related incident reporting – DORA chapter 3 (articles 17 – 23):

ICT-related incident reporting standardizes the process for reporting significant ICT incidents. This second pillar entails developing criteria to classify incidents, setting up procedures to report them to authorities within specified timeframes and promoting information-sharing to enhance collective resilience.

3) Digital operational resilience testing – DORA chapter 4 (articles 24 – 27):

Digital operational resilience testing mandates the regular testing of ICT systems to evaluate their robustness. This third pillar consists of routine testing programs, advanced threat-led penetration testing (where applicable) to simulate real-world attacks, and using test results to improve system resilience.

4) ICT third-party risk management – DORA chapter 5 (articles 28 – 44):

ICT third-party risk management addresses the risks associated with outsourcing ICT services. This fourth pillar specifies that financial entities must perform thorough due diligence before engaging third-party providers, ensure that contractual agreements include resilience and security provisions, continuously monitor third-party performance, and manage risks related to overreliance on a limited number of providers.

5) Information-sharing – DORA chapter 6 (articles 45):

Information-sharing refers to the exchange of threat intelligence and best practices among financial entities and authorities. This fifth pillar promotes participation in collaborative networks for exchanging information and coordinating responses during incidents to improve overall resilience.

In total, DORA consists of 64 articles, 41 of which fall within these five pillars. The other 23 articles do not explicitly address the duties of financial entities. They focus more on background information (scope of application, competent authorities, penalties, delegated acts, transitional and final provisions, and amendments).

2.3.3 The role of RTS and ITS

The main text of DORA is supplemented by important technical detail in a body of secondary legislation, referred to as level 2 regulations. The three European supervisory authorities (ESAs) were jointly appointed to draft these standards. The ESAs consist of the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA).

These technical standards consist of two types:

- Regulatory technical standards (RTS), of which there are eight
- Implementation technical standards (ITS), of which there are two

Development of the RTS and ITS was separated into work on two sets of documents. The first set was submitted to the European Commission (EC) on 17 January 2024. The four RTS documents in this first set were published in the *Official Journal of the European Union* on 25 June 2024, signaling their official adoption. The ITS undergo a different adoption process, so the single ITS in this first set is expected to be adopted by the EC at a later date.

The first set consists of the following documents:

- RTS on ICT risk management framework (part of DORA's first pillar)
- RTS on simplified ICT risk management framework (first pillar)
- RTS on criteria for the classification of ICT-related incidents (second pillar)
- ITS to establish the templates for the register of information (fourth pillar)
- RTS to specify the policy on ICT services performed by ICT third-party providers (fourth pillar)

The second set, which was submitted to the EC in two parts, on 17 July 2024 and 26 July 2024, consists of the following documents:

- RTS on content, timelines, and templates on incident reporting (part of DORA's second pillar)
- ITS on content, timelines, and templates on incident reporting (second pillar)
- RTS on subcontracting of critical or important functions (fourth pillar)
- RTS on oversight harmonization (fourth pillar)
- RTS on threat-led penetration testing TLPT (third pillar)

For links to the latest versions of the RTS and ITS, please see https://www.dnb.nl/dora.

2.3.4 The DORA-NIS2 relationship

Both being key EU legislative frameworks, the NIS2 and DORA not only share in their objective to enhance cybersecurity and operational resilience, but also reference each other. DORA has lex specialis status vis-à-vis NIS2, meaning that DORA serves as a specialized set of rules that take precedence over the more general goals of NIS2.

Some key differences between the two frameworks are that:

- NIS2 targets a much broader sectoral scope; DORA targets the financial sector specifically.
- NIS2 provides overarching generic cybersecurity requirements; DORA provides detailed requirements for the financial sector.
- NIS2 is a directive that must undergo transposition into national law (in the Netherlands, it has been adopted as the Cyberbeveiligingswet); DORA is an EU regulation, which therefore has immediate applicability for all EU member states.

While NIS2 is not a principal topic for this study report, it merits mention. We believe that the DORA in control framework may also be of use for organizations that fall within the scope of NIS2. Because there remains a lack of detailed NIS2 controls, organizations continue to face uncertainty about what to do and implement to achieve NIS2 compliance.

It is notable that NIS2 takes an all-hazards approach in its article 21.1. In this context, an all-hazards approach means organizations must enhance their overall security posture and operational stability through adopting a broad, inclusive strategy for risk management and resilience. This must ensure they are prepared for any potential source of disruption (all hazards), be it in the form of a cyberattacks, natural disaster, technical failure, or another unforeseen event.

In sum, knowing that the requirements in DORA are stricter than those of NIS2, we advise organizations affected by NIS2 regulations to consider implementing the DORA in control framework.

3 DORA's approach

3.1 Principles-based

DORA embodies a shift in regulatory thinking, moving beyond mere compliance toward a principles-based approach to digital resilience. To fully leverage the value of DORA, we recommend organizations use it as a guiding principle for improving operational stability and security, tailored to the specific risk profiles of critical business processes and their supporting ICT systems. This perspective ensures that implementation of the act does not get reduced to a simple compliance exercise, but rather is integrated as a strategic framework for ongoing resilience.

Article 4 of DORA describes the proportionality principle and specifies two ways of applying it.

1. Principles of proportionality are incorporated in specific articles on ICT risk management (DORA chapter 2), whereby microenterprises are allowed to apply simplified requirements.
2. The implementation and application of DORA requirements can be proportionally based on the financial institution's size and overall risk profile as well as the nature, scale, and complexity of services, activities, and operations (via principles-based regulation).

Principles-based regulation emphasizes risk-based adaptability, which allows financial institutions to tailor their risk management and resilience strategies to their unique operational contexts. Unlike prescriptive regulations that dictate specific actions, principles-based regulation encourages entities to take measures and implement controls that are proportional to the risks they face. This approach recognizes the diversity of financial institutions and the varying levels of complexity in their ICT environments.

By adopting a principles-based approach, financial institutions can move beyond a checking-the-boxes mindset of compliance and instead internalize meaningful risk management. This requires a deep understanding of the institution's risk profile, identification of critical or important functions, and assessment of the ICT systems that underpin these functions, while also taking into account the size of an institution.

Tailoring measures to risk profiles

Central to DORA's principles-based approach is the idea that measures and controls should be proportional to the risk profile of business processes and ICT systems. This means that institutions must conduct thorough risk assessments to identify and prioritize their most critical assets and processes. Level of protection, detection, response, and recovery mechanisms should then be aligned with the potential impact of risks on these assets.

For example, a payment processing system that handles a large volume of transactions daily would require more stringent controls and resilience measures compared to a less critical internal administrative system. This targeted approach ensures that resources are allocated efficiently and the most significant risks are clear, thereby enabling the most important risks to mitigated effectively.

Dynamic and continuous improvement

A principles-based approach also emphasizes the dynamic nature of risk management and resilience. Financial institutions must continuously monitor and reassess their risk environments, adapting their controls and measures as new threats and vulnerabilities emerge. An ongoing process of improvement is important for maintaining resilience in a constantly evolving digital landscape.

DORA encourages institutions to foster a culture of continuous learning and adaptation. By regularly testing resilience measures, conducting scenario analyses, and learning from past incidents, financial institutions can

enhance their preparedness and response capabilities. This proactive stance not only fulfills the regulatory expectations of DORA, but also strengthens an institution's overall security posture.

Integrating resilience into business strategy

Viewing DORA as a principles-based framework necessitates integrating digital operational resilience into a broader business strategy. Resilience should not be an afterthought or a separate compliance function, but rather an integral part of strategic planning and decision-making processes. Integration ensures that resilience considerations are embedded in every aspect of the institution's operations, from product development to customer service.

The management body play a critical role in integration. These individuals must champion the importance of resilience, allocate appropriate resources, and ensure that resilience objectives are aligned with the institution's strategic goals. A top-down commitment is essential for creating a resilient organizational culture that prioritizes security and operational stability.

Moving beyond compliance

Ultimately, DORA should be seen as a catalyst for transforming how financial institutions approach digital operational resilience. By embracing its principles-based philosophy, institutions can move beyond the narrow focus of regulatory compliance and adopt a holistic strategic approach to risk management. This shift not only enhances compliance, but also drives operational excellence, innovation, and customer trust.

3.2 Opportunities

While regulatory requirements are often experienced as burdensome, DORA offers financial institutions a significant opportunity to enhance their digital operational resilience. Rather than merely being a compliance mandate, the act provides a strategic framework that can drive improvements other than risk management and ICT operational stability. It can also boost customer trust and overall competitiveness across the financial sector.

Customer trust

For a financial industry that operates in today's digital age, trust and confidence are paramount. By adhering to DORA's stringent resilience requirements, financial institutions can demonstrate their commitment to safeguarding customer assets and ensuring uninterrupted service. This commitment to resilience and security enables trust among customers, partners, and stakeholders. As a result, financial institutions can enhance their reputation, build stronger customer relationships, and create a loyal customer base that values the institution's dedication to digital resilience.

Competitive advantages

Compliance with DORA necessitates the adoption of advanced technologies and innovative solutions to manage ICT risks effectively. Financial institutions that embrace these requirements as an opportunity for digital transformation can gain a competitive edge. By leveraging cutting-edge cybersecurity tools, automated risk management systems, and sophisticated resilience-testing methods, institutions meet regulatory standards while also positioning themselves as leaders in digital resilience. Again, a proactive stance can attract customers who prioritize security and reliability, thereby driving business growth and market differentiation.

Recoverability

DORA offers a crucial opportunity for organizations to enhance their digital recoverability by requiring robust recovery mechanisms and diligent testing to ensure continuous service availability. By complying with DORA's requirements, financial institutions can swiftly restore critical functions, minimize downtime, and protect data integrity during cyber incidents or system failures. This not only ensures regulatory compliance, but also transforms operational resilience into a strategic advantage.

3.3 Challenges

Implementing DORA presents numerous challenges for financial institutions. While DORA's principles-based approach offers flexibility and adaptability, translating its broad requirements into actionable measures can be complex. This can make it difficult for management to navigate and implement effectively.

Multifaceted interpretation

One of DORA's primary challenges is its requirement for interpretation across various domains. Legal experts might focus on the precise wording of the regulation, emphasizing compliance and avoidance of penalties. IT professionals may prioritize technical aspects, such as system security and incident response mechanisms. Business managers are likely to be concerned with maintaining operational efficiency and aligning resilience measures with broader strategic goals. Balancing these perspectives to form a cohesive and actionable strategy can pose challenges for many institutions.

Translating principles into actionable measures

DORA's principles-based nature, while offering flexibility, can also be a double-edged sword. The lack of prescriptive guidelines means that financial institutions must develop their own measures based on their unique risk profiles. However, this requires a deep understanding of both the regulatory requirements and the specific operational risks faced by the institution.

For management, translating these broad principles into specific, actionable measures can be daunting. It involves not only identifying and assessing risks, but also determining the appropriate controls and resilience strategies. This process demands significant expertise and resources, which can be a barrier for many institutions, particularly smaller ones with limited capacity.

Management's role and engagement

Management plays a critical role in driving the implementation of DORA. However, translating technical and legal requirements into strategic business actions is a complex task that requires strong leadership and engagement. Management must not only understand the regulatory landscape, but also be able to articulate the importance of resilience and security to all stakeholders.

Engaging senior management and ensuring their commitment to digital operational resilience is therefore crucial. This includes securing the necessary resources, setting clear priorities, and fostering a culture that values and supports resilience efforts. Without strong leadership and engagement, the implementation of DORA can become disjointed and ultimately ineffective.

Developing a unified framework

Given the diverse interpretations and the need for cross-functional collaboration, developing a unified framework for DORA compliance is essential but nonetheless challenging. A fragmented approach, wherein different departments work in silos, can lead to inconsistencies and gaps in resilience measures.

Financial institutions need a comprehensive framework that integrates legal, IT, and business management perspectives into a cohesive strategy. This framework should facilitate clear communication, consistent interpretation of regulatory requirements, and coordinated action across all levels of the organization.

Wanting to overcome these challenges is precisely why we developed the DORA in control framework. This solution is designed to bridge the gap between the act's high-level principles and the practical, actionable measures required for compliance and resilience. It offers clear controls to help financial institutions navigate the complexities of DORA, ensuring that they can achieve compliance while enhancing their digital operational resilience.

4 DORA in control framework

4.1 Intended purpose

Financial institutions have been struggling with the sheer complexity of Digital Operational Resilience Act (DORA), leading to challenges in implementing effective controls. Through conversations that we held with industry professionals and our extensive market research, a recurring theme emerged: the need for an actionable framework that simplifies DORA's intricate requirements. To this end, the primary objective of the DORA in control framework is to transform the act's legal complexities, along with its 10 RTS and ITS (see section 2.3.3), into clear, actionable strategies for financial institutions.

Ultimately, the framework seeks to make DORA accessible and actionable, ensuring that financial institutions can confidently navigate the regulatory landscape while fortifying their operations against digital threats. In constructing the framework, we kept close to the act's actual requirements and avoided creation of any additional ones to ensure that framework maintains the focus purely on the requirements in the act itself

4.2 How to implement DORA in four steps

DORA implementation can be done successfully through below 4 step approach, which can be integrated in the DORA projects at institutions:

1. When implementing DORA, the first step is to thoroughly assess the organization's critical and/or important functions (article 8.1). This necessitates a comprehensive overview of all key processes and identifying the ICT infrastructure that supports and is essential to the operations of these processes, including third-parties.
2. The next step is to perform a risk assessment on this ICT infrastructure. The assessment helps establish a risk profile and prioritize areas that require attention.
3. Following the risk assessment, the next step would be to deploy the DORA in control framework to conduct a gap analysis. Such analysis identifies where the institution currently stands vis-à-vis DORA requirements and highlights areas where improvements are needed.
4. Based on the gap analysis findings, a final step should be to develop a plan or roadmap, focusing on solutions and mitigating measures to address the identified gaps and root causes and ensure compliance with DORA.

As emphasized in DORA, it is important that the DORA implementation projects are executed directly under responsibility and supervision of the management body. Therefore continuous communication with management is essential to keep them responsible and engaged throughout the process. As included in step 1, equally important is managing relationships with critical third parties, especially since financial institutions increasingly rely on outsourced IT services. The chain of contracting becomes vital for DORA compliance, making it imperative to ensure that all third-party relationships align with the institution's operational resilience and regulatory obligations.

4.3 Constructing the framework

In developing the DORA in control framework, our focus was explicitly on the act's requirements for financial institutions. We therefore excluded any optional requirements or those referring to supervisory, oversight, or background information.

Construction of the framework began with a thorough analysis of the primary (level 1) and secondary (level 2) legislative requirements. Our first step was to distill the complex legal language into a more digestible format for all stakeholders. Once the requirements were put into simpler terms, we employed a mix-and-match process to identify overlapping topics and requirements. This allowed us to consolidate individual requirements into actionable controls that could be logically grouped under recognizable domains, offering improved efficiency when performing a gap assessment and implementation. Each control was cross-

referenced with the specific DORA articles from which it was derived, enhancing both transparency and traceability.

Our process resulted in a framework consisting of eight control domains, 28 sub-domains, and 95 individual controls. For a visualization, see figure 1. During the framework development, IT risk managers, CISOs, and auditors conducted a thorough review process to ensure the quality of the framework. We also created a detailed worksheet to document the translation process, providing a clear audit trail for how the framework evolved from DORA's legal texts to practical controls.

To further support implementation, we integrated the maturity model from the Dutch Central Bank (DNB) Good Practice for Information Security into the framework along with a dashboard that enables users to visualize the implementation and communicate about its progress.

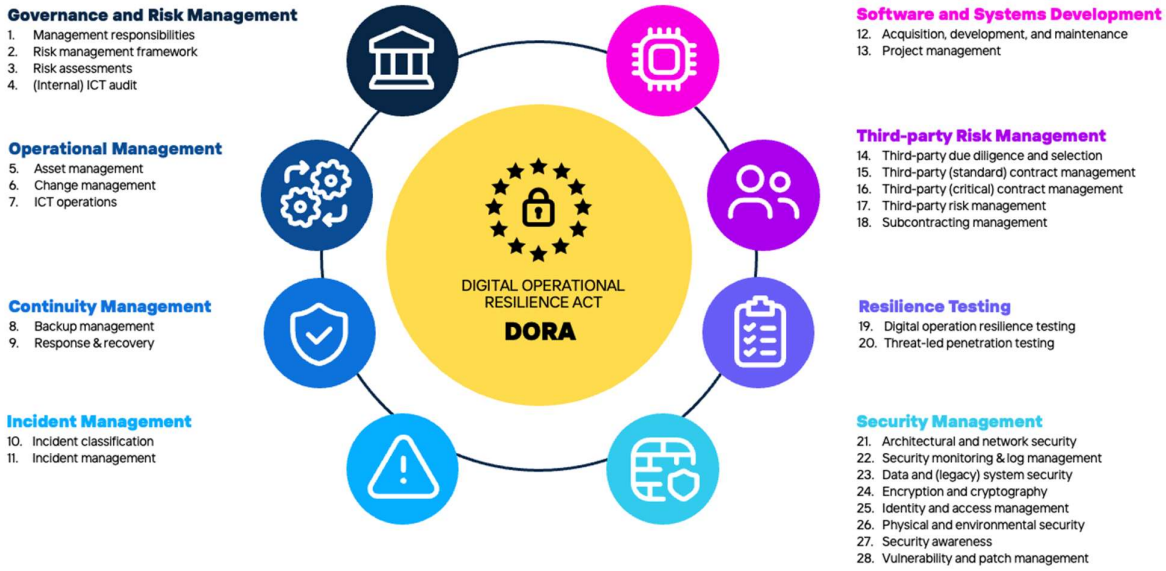

Figure 1: DORA in control framework

4.4 Key features

The DORA in control framework has several key design features tailored to address the act's complexities while providing practical, actionable solutions.

- **Simplified legal interpretation:** One of the framework's most notable features is the translation of DORA's complex legal jargon into more accessible language.
- **Consolidated actionable controls:** The framework consolidates individual DORA requirements into a set of cohesive, actionable controls. Each control is cross-referenced with specific DORA articles, which enhances transparency and facilitates traceability.
- **Integration of the DNB maturity model:** To assist institutions in tracking their progress, the framework incorporates the DNB maturity model from the DNB Good Practice for Information Security.
- **Visual progress dashboard:** The framework incorporates a dashboard to provide a visual representation of implementation progress. This feature offers a clear, intuitive way for institutions to track their advancement and communicate progress to stakeholders, including management and regulatory bodies.
- **Mapping of DNB controls:** The framework includes a mapping of controls in the DNB Good Practice for Information Security to DORA controls, addressing the need to transition from existing standards

to the new regulatory framework. This feature is particularly valuable for institutions accustomed to DNB controls, though is also crucial given the DNB's decision to phase out its own controls in favor of DORA.[4] The mapping helps institutions align their practices with DORA requirements while maintaining continuity in their compliance efforts.

4.5 Engineering perspective

The engineering perspective used to build the DORA in control framework focused on dissecting the act's complexities and utilizing expert input to solve the challenges that arise from it. DORA is principles-based, which offers flexibility but also requires interpretation to enable effective application of those principles. We believe this engineering perspective is crucial for the successful implementation of DORA within financial institutions, as it emphasizes the importance of understanding underlying complexities and root causes while taking a structured and systematic problem-solving approach.

To further enhance the proper implementation of the DORA controls within the institutions, we advise institutions to add a column to document their specific control implementation choices. These should be made based on the institutions context, proportionality and risk profile. To do this from an engineering perspective, we recommend the use of the 5W/1H method. This method consists of asking 6 critical questions for proper problem analysis and solution identification:

- WHAT: What controls are needed? What assets or processes need protection? What are the potential consequences of not doing something?
- WHO: Who is responsible for implementing and maintaining the controls? Who is involved or affected (users, customers, or third parties)?
- WHERE: Where will the controls be implemented (location or asset)? Where should sensitive data and resources be stored securely?
- WHEN: When should the controls be implemented? When will updates and reviews of the controls occur? When will training and education for users take place?
- WHY: Why are these controls necessary? Why were these specific controls chosen? Why did existing measures fail?
- HOW: How will the controls be implemented and enforced? How will the effectiveness of the controls be measured? How will issues or breaches be handled?

4.6 Mapping toward the DNB Good Practice for Information Security

In the Netherlands, many financial institutions are used to implement and report on cyber security based on the DNB Good Practice for Information Security from the Dutch Central Bank[5]. Therefore, the DORA in control framework is mapped to the controls in the DNB Good Practice for Information Security 2023. This mapping shows that 44% of the DORA controls are already accounted for in the DNB controls, while 41% are partly mapped, and 15% are completely new. For a visualization, see figure 2.

[4] https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2024/dora-17-januari-2025-nadert-sneller-dan-u-denkt/
[5] https://www.dnb.nl/media/vskni24i/good-practice-ib-2023.pdf

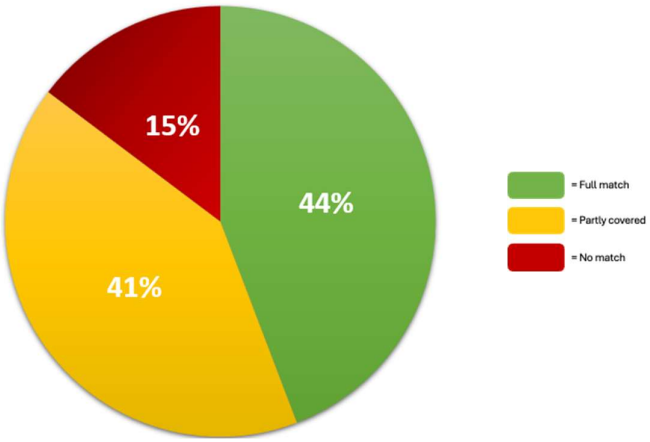

Figure 2: Mapping result between DORA in control framework and DNB Good Practice for Information Security 2023

DORA controls that are mostly covered by DNB controls (50%+ overlap) fall within the following domains:

1) Software and systems development
2) Operational management
3) Resilience testing

Largest gaps in correspondence between DORA controls and DNB controls fall within the following domains:

1) Continuity management
2) Security management
3) Third-party risk management
4) Incident management

For a visualization of how all eight domains overlap, please see figure 3.

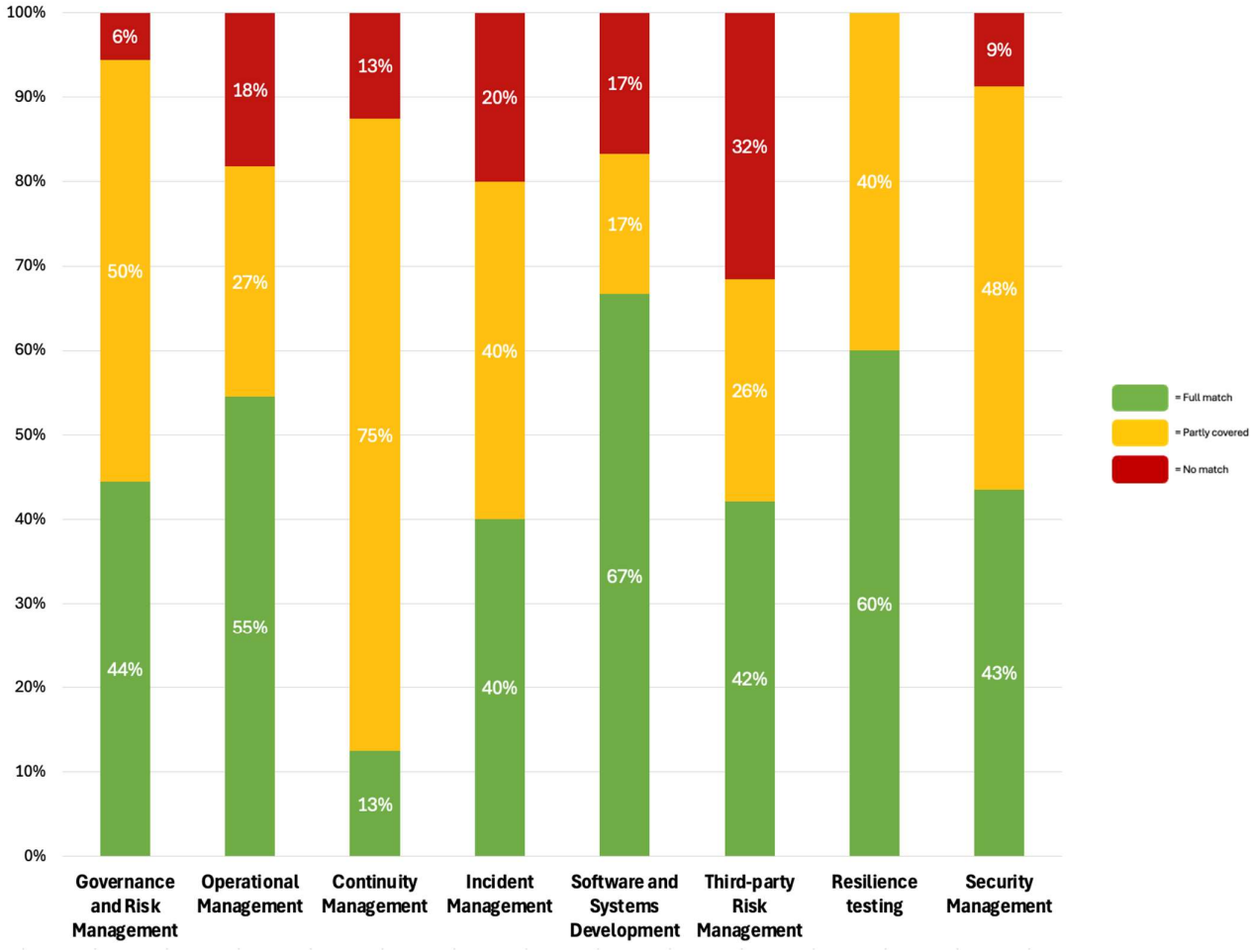

Figure 3: DNB Good Practice for Information Security 2023 mapping to the DORA in control framework per domain

4.7 The control framework

Governance and Risk Management

GRM.1 Management Responsibilities

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Governance and Risk Management	1	**Management Responsibilities**	1.1	**Governance of ICT risk**	The Management body shall take ultimate responsibility for effectively managing all ICT risks of the financial entity. As such, the management body periodically (e.g. annually) reviews and approves: - Policies related to the availability, authenticity, integrity, and confidentiality of data, including the policy on arrangements with ICT third-party service providers (see control 2.1). - The roles, responsibilities and goverance arrangements for ICT risk management (including those related to ICT third-party arrangements), including the continuous monitoring thereof. - the policy on arrangements with ICT third-party service providers and stays informed about third-party arrangements, services provided, planned material changes regarding third- party service providers, and understand the impact of these changes on critical and important functions of the entity (including risk assessment results).	5.1 5.2 5.3 5.4 6.8 13.4 13.7
Governance and Risk Management	1	**Management Responsibilities**	1.2	**Knowledge of the Management Body**	The Management body shall ensure that it is kept up to date with sufficient knowledge and skills to understand and assess ICT risks and operations (e.g. through periodic trainings).	
Governance and Risk Management	1	**Management Responsibilities**	1.3	**Digital Operational Resilience Strategy**	The Management body shall set and approve the digital operational resilience strategy and periodically update when needed. The digital operational resilience strategy must: - Set out how the risk management framework will be implemented. - Elaborate on the alignment between the risk management framework and the business strategy and objectives. - Establish the ICT risk tolerance level (based on risk appetite) and the impact tolerance level for ICT disruptions. - Include clear security objectives, including Key Performance Indicators (KPIs) and risk metrics. - Elaborate on the ICT reference architecture and any changes needed to reach specific business objectives. - Outline the mechanisms in place to detect ICT-related incidents - Contain evidence to prove the current digital operational resilience situation (e.g. based on the number of major ICT-related incidents and the effectiveness of preventive measures. - Contain how the digital operational resilience testing is implemented (see controls under 19 and 20). - Outline the communication strategy in case of incidents (see 11.3) The Management body shall allocate and review the budget required for resources to fulfill the digital operational resilience needs of the entity. Ensure monitoring is arranged on the the effectiveness of the implementation of the digital operational resilience.	
Governance and Risk Management	1	**Management Responsibilities**	1.4	**Business Continuity Oversight**	The Management body reviews and approves periodically (e.g. annually) the ICT business continuity policy and the ICT response and recovery plans.	
Governance and Risk Management	1	**Management Responsibilities**	1.5	**Audit Plan Approval and Review**	The Management body reviews and approves periodically (e.g. annually) internal ICT audit plans, ICT audits, and material modifications to the audits.	

GRM.2 Risk Management Framework

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Governance and Risk Management	2	**Risk Management Framework**	2.1	**Protection Measures**	Implement policies and procedures to protect all information, ICT assets, and relevant physical ICT components and infrastructures. At least the following policies shall be established, maintained and approved by the Management body. - Security policy - Human resources policy - Encryption and cryptographic control policy - Identity and access management (IAM) policy - Change management policy - Network security policy - ICT operating policies and procedures - Communication policy - Vulnerability and patch management policy - Back up policy - Project management policy - Physical and environmental security policy - Business continuity policy with response and recovery plans (including testing plans) - ICT third-party service providers management policy - Operations of ICT assets (ensuring network security, protect against intrusions and data misuse and defining how the entity operates, monitors, controls, and restores ICT assets, including the documentation of ICT operations)	6.1 6.2 6.3 6.4 6.5 6.7 8.1 9.1 9.4 11.1 11.3 11.6 12.1 12.2 12.3 13.3 13.5 13.7 24.1 28.2 28.3 1.1 (RTS RM) 2.1 (RTS RM) 2.2 (RTS RM) 3.1 (RTS RM) 3.1 (RTS TPPM) 3.2 (RTS TPPM) 3.3 (RTS TPPM) 3.4 (RTS TPPM) 3.6 (RTS TPPM) 3.7 (RTS TPPM) 4.1 (RTS TPPM) 7.1 (RTS TPPM) 7.2 (RTS TPPM) 8.1 (RTS RM) 8.2 (RTS RM)
Governance and Risk Management	2	**Risk Management Framework**	2.2	**Critical and Important Functions**	Identify, classify and adequately document all critical and important functions. This process involves determining which functions are essential for the entity's operational stability and continuity. Review as needed, and at least yearly, the adequacy of this classification.	
Governance and Risk Management	2	**Risk Management Framework**	2.3	**Clear Segregation of Duties (SoD)**	Establish Segregation of Duties (SoD) with regard to risk management functions, following the three lines of defence model or internal risk management and control model.	
Governance and Risk Management	2	**Risk Management Framework**	2.4	**ICT Risk management framework**	A sound, comprehensive and well-documented ICT risk management framework is in place. Which as goal to address all ICT risks properly and ensure a high level of digital resilience. The reponsibility for risk management is properly assigned to a control function.	
Governance and Risk Management	2	**Risk Management Framework**	2.5	**Annual Framework Review and Audit Process**	The effectiveness of the risk management framework is monitored based on the risk exposure over time to critical or important business functions. Implement a reviewing and auditing process, with a minimum yearly review of the framework, triggered by major ICT incidents, regulator instructions, or major audit findings.	
Governance and Risk Management	2	**Risk Management Framework**	2.6	**Third-Party (Multi-vendor) Risk Management Program**	Maintain a comprehensive third-party risk management program which includes: - A register of information related to the use of thirdparty service providers, especially those supporting critical or important functions (see also control 17.3). - Put in place a policy on the management of ICT third-parties, including the criteria for determining the criticality of service providers and the internal responsibilities for managing third-parties. - Ensuring that senior management reviews the policy and designate a member to monitor relations with the third-parties and the contractual arrangements. - A multi-vendor strategy, if deemed relevant, showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of ICT third-party service providers.	

GRM.3 Risk Management Framework

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Governance and Risk Management	3	Risk Asesssments	3.1	Risk Assessment	Identify all sources of ICT risk on a continuous basis, including risk exposure to and from other entities. Gather information, assess, and review at least on a yearly basis the cyber threats and ICT vulnerabilities relevant to business functions and assets. Evaluate the (potential) impact of these threats and vulnerabilities on the assets.	8.2 8.3 8.7 8.4 13.1
Governance and Risk Management	3	Risk Asesssments	3.2	Major change risk assessment	Perform a risk assessment upon each major change in the network, IT infrastructure, and the processes or procedures affecting business functions and assets.	
Governance and Risk Management	3	Risk Asesssments	3.3	Legacy Systems risk assessment	Conduct specific risk assessments on all legacy ICT systems, applications, or systems at least yearly. Perform assessments before and after connecting legacy ICT systems, applications, or systems.	

GRM.4 (Internal) ICT Audit

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Governance and Risk Management	4	(Internal) ICT Audit	4.1	Audit approach and frequency	The Internal audit department shall conduct audits on the following domains: - Risk management framework, policies, related processes, and procedures - ICT Response and recovery plans - ICT Third-party service providers Adjust audit frequency and focus based on the entity's ICT risk profile.	6.6 11.3 13.7 28.6 3.8 (RTS TPPM) 8.1 (RTS TPPM) 8.2 (RTS TPPM) 8.3 (RTS TPPM)
Governance and Risk Management	4	(Internal) ICT Audit	4.2	Auditor requirements	Ensure that the internal audit staff possess sufficient ICT risk knowledge, skills, and expertise to perform the audits. Also, ensure the independence of the audit function.	
Governance and Risk Management	4	(Internal) ICT Audit	4.3	Audit findings	Establish a follow-up process for audit findings, including rules for timely verification and remediation of critical findings. Maintain a continuous learning and improvement process based on risk assessment results, resilience testing, (cyber) incidents, and testing of business continuity plans. The results of this process shall be reported annually by senior ICT staff to the management body. The format and content of the review report shall meet the requirements stated in Chapter 5 (Article 27) of RTS RM.	
Governance and Risk Management	4	(Internal) ICT Audit	4.4	Reliance Third-Party Assurance and Certifications	Use, where appropriate, third-party certifications, third-party or internal audit reports made available by the ICT third-party service provider, or own audit reports to confirm adherence of contractual requirements on information access, inspection, audit, and ICT testing with the third-party. Rely on third-party certifications and audit reports from ICT third-party service providers only if the following specific conditions are met: the audit plan is aligned with contractual arrangements, the audit scope is comprehensive and covers identified systems and key controls, ongoing assessment of certification/report content are performed and validated, key systems and controls are covered in future versions of the certification or audit report, there is confidence in the certifying/auditing party's capabilities, certifications/audits adhere to recognized professional standards, the right to request scope expansion is covered in the contract, and right to perform discretionary audits is retained.	

Operational Management

OM.5 Asset Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Operational Management	5	**Asset Management**	5.1	**Resilient Systems**	Use and maintain ICT systems, protocols, and tools that are up to date and: - Tailored to the magnitude of ICT operations - Reliable - Equipped with sufficient capacity to accurately process data and to deal with peak orders, message or transaction volumes as needed - Technologically resilient to deal with additional processing needs under stressed market conditions or other adverse market conditions	7 8.1 8.5 8.6 4.1 (RTS RM) 4.2 (RTS RM) 5.1 (RTS RM) 5.2 (RTS RM)
Operational Management	5	**Asset Management**	5.2	**Inventory Management**	Keep an inventory of (ICT) assets, monitor their life-cycle and update it periodically and upon every major change in the network, the IT infrastructure, and processes and procedures supporting business functions. Keep records of the following for each ICT asset: unique identifier, location (physical or logical), asset classification, identity of asset owner, information for specific risk assessment on legacy systems, business functions or services supported, business continuity requirements (e.g., RTO, RPO), exposure to external networks, including the internet, links and interdependencies among assets and business functions using each asset, and the end dates of the ICT third-party service provider's regular, extended and custom support services after which it is no longer supported by its supplier or by an ICT third-party service provider. Ideally, inventory management is perfomed in an automated and continuous fashion.	
Operational Management	5	**Asset Management**	5.3	**Asset Classification and Documentation**	Identify, classify and document all ICT-supported business functions, including the assets supporting them, and detail the roles and dependencies of these assets in relation to ICT risk. Additionally, identify and document all ICT-supported business functions dependent on ICT third-party service providers, and identify the services provided by third-party providers that support critical or important business functions. Make a mapping of critical (ICT) assets based on a criticality assessment, which must include network resources, hardware equipment, and resources on remote sites. This mapping should also incorporate the configuration of assets and their links and interdependencies with other assets. The criticality assessment should follow clear criteria to evaluate the ICT risk related to business functions, taking into account the potential impact of confidentiality, integrity, and availability losses. Review the adequacy of this classification and documentation at least on a yearly basis, ensuring it meets the requirements for maintaining accurate and up-to-date asset records.	

OM.6 Change Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Operational Management	6	Change Management	6.1	Change Procedures	Ensure that all changes to software, hardware, firmware components, and systems, along with security parameters, are appropriately placed and scoped. Document and communicate change details, including the purpose and scope of the change, the implementation timeline, and expected outcomes. Define clear roles and responsibilities to ensure that changes are defined, planned, transitioned, tested, and finalized in a controlled manner. Additionally, establish effective quality assurance procedures. Implement mechanisms to maintain independence between the functions that approve changes and those responsible for requesting and implementing them.	8.1 (RTS RM) 8.2 (RTS RM) 17.1 (RTS RM) 17.2 (RTS RM)
Operational Management	6	Change Management	6.2	Security Requirements	Identify the potential impact of a change on existing security measures and assess whether additional security measures are required for its implementation. Verify that security requirements have been met for all implemented changes. Establish fallback procedures and assign responsibilities for aborting changes or recovering from changes not successfully implemented.	
Operational Management	6	Change Management	6.3	Emergency Change Management	Define procedures for documenting, reevaluating, assessing, and approving the implementation of emergency changes, including workarounds and patches.	
Operational Management	6	Change Management	6.4	OTAP Implementation	Ensure segregation of production environments from development, testing, and other non-production environments, encompassing all components of an environment. This also includes requirements to conduct the development and testing in production environments. Ensure that the instances in which testing is performed in production environment are clearly identified, justified, for limited periods of time approved by the relevant function.	

OM.7 ICT Operations

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Operational Management	7	ICT Operations	7.1	ICT Monitoring	Develop, document and implement capacity and performance management procedures to identify capacity requirements of their ICT systems and apply resource optimisation and monitoring procedures to maintain and improve the availability of data and ICT systems and efficiency of ICT systems and prevent ICT capacity shortages.	8.1 (RTS RM) 8.2 (RTS RM) 9.1 (RTS RM) 9.2 (RTS RM) 12.2 (RTS RM)
Operational Management	7	ICT Operations	7.1	Clock Synchronization Standardization	Ensure clock synchronization of all ICT systems to a single reliable reference source time.	
Operational Management	7	ICT Operations	7.1	System Management and Security	Provide system descriptions that encompass secure installation, maintenance, configuration, and deinstallation/disposal of ICT assets. This includes the management of assets, both automated and manual, and the identification and control of legacy ICT systems.	
Operational Management	7	ICT Operations	7.1	Error Handling and Recovery	Establish guidelines for handling errors, including support and escalation contacts, as well as external support contacts in case of unexpected operational or technical issues. Define the procedures for ICT system restart, rollback, and recovery to be used in the event of an ICT system disruption. Ensure the contact details are available in case systems are unavailable as well.	

Continuity Management

CM.8 Backup Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Continuity Management	8	**Backup Management**	8.1	**Backup Policy**	Define backup policies aimed at ensuring minimum downtime, limited disruption, and loss, and put in place restoration and recovery procedures. Specify the scope of the data subject to backups and the minimum frequency of backups, based on the criticality or confidentiality of data. Determine a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) based on data criticality and overall impact on market efficiency to ensure that service levels are met in extreme scenarios.	12.1 12.2 12.3 12.6 12.7
Continuity Management	8	**Backup Management**	8.2	**Restore Procedures**	Ensure that the activation of backup systems will not jeopardize the security of ICT systems or the availability, authenticity, integrity or confidentiality of data. For example through the execution of periodic restore tests based on the backup, restoration, and recovery procedures. Ensure that when restoring backup data using self-managed systems, that systems are used that are both physically and logically segregated from the source system to ensure protection. Furthermore, the backup systems shall be securely protected from any unauthorized access or IT corruption and allow for timely restoration. Institutions must validate that the highest level of data integrity is maintained when restoring backups. **Additionally 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. **Additionally for data reporting service providers*:** the 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. *For definition of DRSP see: https://www.esma.europa.eu/esmas-activities/markets-and-infrastructure/data-reporting-services-providers	

CM.9 Response and Recovery

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Continuity Management	9	Response and Recovery	9.1	Business Continuity Policy	Establish an ICT business continuity policy that enables the continuity of critical or important functions, ensures rapid response to incidents, facilitates the resumption of activities, deployment of containment measures, activation and deactivation of response and recovery procedures, estimation of impact, damage, and losses, and provides clear communication to relevant stakeholders. Regularly review the business continuity policy and make necessary adjustments to enhance effectiveness. **Refer to Articles 24.2-4 of the RTS RM for specific requirements for Central counterparties, Trading venues, and Central security depositories.**	11.1 11.2 11.4 11.5 11.6 11.7 11.8 11.9 11.10 12.5 24.1 (RTS RM) 24.2 (RTS RM) 24.3 (RTS RM) 24.4 (RTS RM) 25.1 (RTS RM) 25.2 (RTS RM) 25.3 (RTS RM) 25.4 (RTS RM) 25.5 (RTS RM) 25.6 (RTS RM) 26.1 (RTS RM) 26.2 (RTS RM) 26.3 (RTS RM) 26.4 (RTS RM)
Continuity Management	9	Response and Recovery	9.2	Crisis Management	Formulate and maintain a crisis management team tasked with overseeing and coordinating actions during a crisis or major disruption. Regularly review recovery/response plans. Make necessary adjustments to enhance effectiveness.	
Continuity Management	9	Response and Recovery	9.3	Record Keeping	Keep detailed records of activities conducted before, during, and after disruptions, including actions taken and outcomes. Maintain an estimation of aggregated annual costs and losses resulting from major disruptions. This information shall be reported to the regulator upon their request.	
Continuity Management	9	Response and Recovery	9.4	Business Impact analysis	Perform a comprehensive Business Impact Analysis (BIA) of exposures to severe business disruptions. The BIA should be done by means of quantitative and qualitative criteria, using internal and external data and scenario analysis, as appropriate. The BIA shall consider the criticality of identified and mapped business functions, support processes, third-party dependencies and information assets, and their interdependencies. Financial entities shall ensure that ICT assets and ICT services are designed and used in full alignment with the BIA, in particular with regard to adequately ensuring the redundancy of all critical components.	
Continuity Management	9	Response and Recovery	9.5	Response and Recovery	Establish comprehensive response and recovery plans encompassing short-term and long-term recovery options. These plans must thoroughly identify potential scenarios and shall duly take into account scenarios of cyber-attacks, switchovers, degradation of critical function provision, premises failure, breakdowns in ICT assets or communication infrastructure, staff unavailability, natural disasters and the impact of climate change, pandemic situations, physical attacks, insider threats, political or social instability, and power outages. Additionally, these plans must incorporate alternative options in cases where primary recovery measures are impractical in the short term due to factors such as cost, risks, logistics, or unforeseen circumstances. Address potential failures of key ICT third-party service providers into the plans.	
Continuity Management	9	Response and Recovery	9.6	Testing and Assessment	Regularly test ICT business continuity, response, and recovery plans, particularly in collaboration with third-party service providers supporting critical or important functions. Testing should take into account the financial entity's BIA and the ICT risk assessment and occur on a yearly basis and whenever there are significant changes to systems supporting critical or important functions. Tests must be based on realistic scenarios and encompass scenarios like cyber attacks, insolvency or failure of the third-party, backup restores, and switchover between primary and redundant processing sites. The testing shall verify whether at least critical or important functions can be operated appropriately, for a sufficient period of time and whether the normal functioning (of the business process) may be restored. Conduct testing of crisis communication plans to ensure effective communication strategies during a crisis or major disruption. Document test results and report any identified deficiencies resulting from the tests to the management body. **Refer to Articles 24.2-3 of the RTS RM for the specific requirements for Central counterparties and Central security depositories.**	

Incident Management

IM.10 Incident Classification

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Incident Management	10	Incident Classification	10.1	Incident Classification Criteria	Classify ICT-related incidents based on their impact using the following criteria: number of clients/customers or financial counterparts affected, number of transactions affected, reputational damage, duration of the incident and downtime of services, geographical spread of the incident, data loss in relation to the CIA-triad, criticality of the services affected, and the overall economic impact of the incident. An incident is considered major if (1) any malicious unauthorised access to network and information systems is identified, which may result to data losses or (2) the thresholds of two additional criteria are met (refer to the DORA RTS IM (Major Incidents) sheet for the thresholds). Also, take into account recurring incidents, where recurring incidents are considered major when (1) the incidents have occurred at least twice within 6 months, (2) the incidents have the same apparent root cause, (3) the incidents collectively categorise as a major incident.	18.1 18.2 1 (RTS IM) 2 (RTS IM) 3 (RTS IM) 4 (RTS IM) 5 (RTS IM) 6 (RTS IM) 7 (RTS IM) 8 (RTS IM) 9 (RTS IM) 10 (RTS IM) 11 (RTS IM) 12 (RTS IM) 13 (RTS IM) 14 (RTS IM) 15 (RTS IM) 16 (RTS IM)
Incident Management	10	Incident Classification	10.2	Cyber Threat Classification Criteria	Classify significant cyber threats. A threat is considered significant if it has a high probability of materialisation, could meet any of the criteria that classify as a 'major incident' when materialised, and when it could affect or could have affected critical or important functions of the financial entity, or could affect other financial entities, third party providers, clients or financial counterparts.	

IM.11 Incident Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Incident Management	11	**Incident Management**	11.1	**Incident Management Process**	Implement an incident management process to detect, manage, and report ICT incidents. This includes incident response procedures to mitigate impacts and ensure timely restoration of services. Assign specific roles and responsibilities for various incident scenarios. Also, establish a list of contacts with internal functions and external stakeholders that are directly involved in ICT operations security, including on detection and monitoring cyber threats, detection of anomalous activities and vulnerability management. Establish early warning indicators for potential incidents and incident triggers upon the occurance of malicious activity, data losses, adverse impact detected on financial entity's transactions and operations, systems and network unavailability, problems reported by users of the financial entity, and incident notifications from an third-party service provider detected in the systems and networks of the third-party service provider and which may affect the financial entity. Identify, document, and address incident root causes. Conduct post-ICT-related incident reviews after major disruptions. Analyze causes, evaluate response promptness and quality, and assess incident escalation and communication effectiveness.	13.2 17.1 17.2 17.3 19.1 19.3 19.4 22.1 (RTS RM) 23.1 (RTS RM) 23.5 (RTS RM) 2.1 (RTS/ITS MIR) 3.1 (RTS/ITS MIR) 4.1 (RTS/ITS MIR) 5.1 (RTS/ITS MIR) 6.1 (RTS/ITS MIR) 6.2 (RTS/ITS MIR) 6.3 (RTS/ITS MIR) 6.4 (RTS/ITS MIR) 6.5 (RTS/ITS MIR) 7.1 (RTS/ITS MIR)
Incident Management	11	**Incident Management**	11.2	**Incident Tracking**	Develop procedures to identify, track, log, categorize, and classify ICT-related incidents based on priority, severity, and criticality of impacted services. Maintain records of all ICT-related incidents and significant cyber threats. Implement a monitoring process to track incidents and cyber threats.	
Incident Management	11	**Incident Management**	11.3	**Incident Communication and Reporting**	Create communication plans to inform both internal (staff, senior management) and external (clients/customers, financial counterparts) stakeholders on incidents. Inform affected customers promptly upon awareness of an incident that impacts them. Provide details on the incident and outline mitigating measures taken and planned. Report major incidents to the regulator, involving three stages: 1) initial notification upon discovering the incident (within 4 hours from the moment of classification of the incident as major, but no later than 24 hours from the time of detection of the incident) , 2) intermediate report on incident developments (within 72 hours from the submission of the initial notification even where the status or the handling of the incident have not changed, or when regular activities have been recovered), and 3) the final report with the root cause analysis and follow-up actions (no later than one month from the submission of the latest updated intermediate report). Also provide notifications to the regulator on significant cyber threats. The incident reports and notifications on cyber threats shall follow the content guidelines defined in the corresponding RTS/ITS.	

Software and Systems Development

SSD.12 Acquisition, Development, and Maintenance

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Software and Systems Development	12	**Acquisition, Development, and Maintenance**	12.1	**Policy Framework**	Establish and maintain a policy governing the acquisition, development, and maintenance of ICT systems. Implement security practices and methodologies throughout the acquisition, development, and maintenance lifecycle. Define functional and non-functional requirements for ICT systems, including security aspects. Obtain approval from relevant business functions and asset owners in accordance with internal governance.	16.1 (RTS RM) 16.2 (RTS RM) 16.3 (RTS RM) 16.4 (RTS RM) 16.5 (RTS RM)
Software and Systems Development	12	**Acquisition, Development, and Maintenance**	12.2	**Environment Risk Mitigation Measures**	Put in place measures to mitigate the risk of unintentional alteration or intentional manipulation during development, maintenance, and deployment in production. Protect the integrity and confidentiality of data in non-production environments. Store only anonymized, pseudonymized, or randomized production data. Production data that are not anonymized, not pseudonymized or not randomized may be stored only for specific testing occasions, for limited periods of time and following the approval by the relevant function and, for financial entities other than microenterprises, the reporting of such occasions to the ICT risk management function.	
Software and Systems Development	12	**Acquisition, Development, and Maintenance**	12.3	**Systems Testing Procedures**	Develop and follow procedures for testing and approval of all ICT systems before use and after maintenance. Determine testing level based on criticality of the business functions and ICT assets. Design and implement testing procedures to verify that new ICT systems are adequate to perform as intended, including the quality of the software developed internally. Perform security testing of software packages no later than the integration phase.	
Software and Systems Development	12	**Acquisition, Development, and Maintenance**	12.4	**Source Code Reviews**	Conduct source code reviews encompassing static and dynamic testing, for the purpose of acquisition, development and maintenance of ICT-systems. Include security testing for internet-exposed systems. Identify and address vulnerabilities and anomalies in the source code and put in place plans to mitigate them. Monitor mitigation efforts. Implement controls to safeguard the integrity of source code, whether developed in-house or by a third-party service provider. Analyze and test source code and proprietary software provided by third-party service providers or from open-source projects for vulnerabilities.	

SSD.13 Project Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Software and Systems Development	13	Project Management	13.1	ICT Project Management Practices	Ensure effective management of ICT projects related to acquisition, maintenance, and, where applicable, development of ICT systems, through a project management policy. The ICT project plan shall include: clear project objectives, project governance structure, roles and responsibilities, defined timeframe and steps, key project milestones, and change management requirements. Specify requirements for project team members, ensuring the inclusion of staff from business activities or functions impacted by the project. Team members must possess the knowledge to ensure the secure and successful project implementation. Establish reporting requirements, including periodic reporting on the establishment and progress of projects impacting critical or important functions, along with their associated risks. Reporting shall be done periodically and, where necessary, on an eventdriven basis, considering the importance and size of the ICT projects and the project risk assessment.	15.1 (RTS RM) 15.2 (RTS RM) 15.3 (RTS RM) 15.4 (RTS RM) 15.5 (RTS RM)
Software and Systems Development	13	Project Management	13.2	Project Risk Management	Perform a risk assessment of the ICT project. Conduct testing of all project management requirements, including security requirements. Establish an approval process for deploying to the production environment.	

Third-party Risk Management

TPRM.14 Third-party Due Diligence and Selection

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Third-party Risk Management	14	Third-party Due Diligence and Selection	14.1	Suitability Criteria	Ensure that the third-party service provider has the business reputation, sufficient abilities, expertise and adequate financial, human and technical resources, information security standards, appropriate organisational structure (including risk management and internal controls) and, if applicable, the required authorisation(s) or registration(s) to provide ICT services supporting the critical or important functions in a reliable and professional manner.	3.5 (RTS TPPM) 3.9 (RTS TPPM) 5.2 (RTS TPPM) 6.1 (RTS TPPM) 6.2 (RTS TPPM) 6.3 (RTS TPPM)
Third-party Risk Management	14	Third-party Due Diligence and Selection	14.2	Selection Criteria	Take the following into account when selecting and assessing the service provider: audits conducted by the financial entity or on its behalf, third-party certifications, independent audit reports, internal audit function reports, and publicly available information. Confirm adherence to ethical, social, human, and environmental (sustainability) principles, encompassing appropriate working conditions including the prohibition of child labour. Assess if the service provider operates in a third country and evaluate if this practice heightens operational, reputational, or sanctions-related risks. Secure consent from the service provider for effective audit conduct, both onsite and by designated parties, including auditors from the financial entity, external (third-party auditors), and by competent authorities (such as the regulator). Verify if the service provider intends to engage ICT sub-contractors for substantial portions of their services.	

TPRM.15 Third-party (Standard) Contract Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Third-party Risk Management	15	Third-party (Standard) Contract Management	15.1	Termination Rights and Conditions	Define explicit termination rights including significant breaches of laws, regulations, or contract terms, material changes in third-party risks, demonstrated ICT weaknesses, and regulator oversight constraints. Set provisions for ensuring access, recovery, and return of data in an easily accessible format in cases of termination, insolvency, resolution, or discontinuation of the service provider's business operations.	28.7 30.1 30.2 3.9 (RTS TPPM)
Third-party Risk Management	15	Third-party (Standard) Contract Management	15.2	Service Level Management	Define clear and measurable service level descriptions outlining expected performance and quality standards. Ensure that the service provider provides a comprehensive description of all functions and ICT services that are offered, including any sub-contracting arrangements. Establish arrangements ensuring appropriate levels of data protection in line with regulatory requirements.	
Third-party Risk Management	15	Third-party (Standard) Contract Management	15.3	Service Locations and Data Processing	Specify service locations and data processing sites. Require timely notification of any intended changes to these locations.	
Third-party Risk Management	15	Third-party (Standard) Contract Management	15.4	Cooperation in Incident Response	Oblige the ICT third-party service provider to fully cooperate with the regulator and provide necessary assistance in the event of an incident related to the provided service.	
Third-party Risk Management	15	Third-party (Standard) Contract Management	15.5	Participation in Security Awareness Programs	Specify conditions for the participation of the service provider in security awareness and resilience programs/trainings.	

TPRM.16 Third-party (Critical) Contract Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Third-party Risk Management	16	Third-party (Critical) Contract Management	16.1	(Critical) Service Level Management	Ensure the contract with ICT third-party service provider delivering critical or important services encompasses comprehensive service level descriptions, including updates and detailed reporting (both quantitative and qualitative). Evaluate the service provider's compliance with performance and quality standards by reviewing reports on activities and services, incident reports, security and business continuity measures, and testing. Assess performance using key performance indicators, key control indicators, audits, self-certifications, and independent reviews. Receive relevant information from the service provider regarding their activities and services and ensure timely notification and response to incidents. Conduct independent reviews and compliance audits with legal and regulatory requirements and policies. Specify notification periods for any material changes that may impact the entity or agreed service levels.	30.3 9.1 (RTS TPPM) 9.2 (RTS TPPM) 4.1 (RTS SCM) 4.2 (RTS SCM) 7.1 (RTS SCM)
Third-party Risk Management	16	Third-party (Critical) Contract Management	16.2	Contractual Clauses	Secure rights for continuous performance monitoring, including unrestricted rights to access, inspection, and audit. This encompasses alternative assurance levels, cooperation with regulator inspections, and full disclosure of audit scope, procedures, and frequency. Include a mandatory transition period upon termination, allowing the service provider to continue services during migration, affording the entity time to transition to another provider or in-house solutions based on service complexity. Mandate the implementation and testing of business contingency plans and the establishment of a security management system by the service provider. Require the service provider's participation in the entity's (advanced) testing program (TLPT), where required.	
Third-party Risk Management	16	Third-party (Critical) Contract Management	16.3	Third-party Critical Subcontracting Management	Delineate critical and important ICT services in contracts with third-party ICT service providers, specifying conditions for subcontracting. Require continual monitoring of subcontracted services supporting critical functions to ensure compliance with contractual obligations. Detail monitoring and reporting responsibilities of the third-party service provider to the financial entity, including risk assessments related to subcontractor locations and data ownership. Mandate incident response and business continuity plans for subcontractors, along with adherence to specified service levels and security standards. Ensure subcontractors grant the same audit and access rights to the financial entity as the primary service provider. Retain termination rights for the financial entity in cases of unauthorized subcontracting or failure to meet agreed-upon service levels. Implement changes relative to contractual agreements as soon as possible and document the planned timeline for the implementation.	

TPRM.17 Third-party Risk Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Third-party Risk Management	17	Third-party Risk Management	17.1	Third-party Risk Management	Manage third-party risks proportionate to dependency nature, service-related risks, and impact on entity's continuity and availability in case of disruption. Implement a policy for critical function ICT services provided by third-party service providers, considering the location of the service provider (or its parent company), the level of assurance regarding the service providers' risk management framework (including risk mitigation and business continuity measures), the nature of the data shared with the service provider, the location of data processing and storage, group affiliation of the service provider, and the potential impact of the risks and disruptions on the continuity and availability on the activities of the entity. Test response and recovery of critical function-supporting services provided by third parties.	8.5 11.4 28.1 28.3 28.4 28.5 28.6 28.8 29.1 29.2 3.9 (RTS TPPM) 4.1 (RTS TPPM) 10.1 (RTS TPPM)
Third-party Risk Management	17	Third-party Risk Management	17.2	Pre-Contract Risk Assessment	Perform pre-contract risk assessment. This assessment must assess if: the contract covers services supporting critical or important functions, a service provider is easily replaceable, the risks of sub-contracting are covered, the risks of outsourcing service to a third-country are covered, the risks of bankruptcy are covered on the side of the service provider, supervisory conditions for contracting are met, all contractual risks are identified and assessed (e.g., to cover for ICT concentration risks), the service provider is suitable, and if there are conflicts of interest. Assess service provider resources for ensuring entity compliance with all legal and regulatory requirements.	
Third-party Risk Management	17	Third-party Risk Management	17.3	Register of Information	Maintain a comprehensive register of information related to contractual arrangements with third-party service providers, distinguishing those supporting critical/important functions. Ensure that the register is in line with all mandatory fields as defined in the ITS on the register of information.	
Third-party Risk Management	17	Third-party Risk Management	17.4	Contractual Requisites	Only contract with service providers meeting appropriate information security standards (e.g., ISO 27001, SOC, PCI-DSS, etc.) appropriate to the criticaly of services delivered. Determine audit frequency for service providers, ensuring auditors possess requisite skills and knowledge for complex services	
Third-party Risk Management	17	Third-party Risk Management	17.5	Exit strategies	Develop and periodically test exit strategies and plans, considering risks related to third-party service providers, including potential failure, service quality deterioration, business disruption, and termination of contractual arrangements. Ensure that the exit plan is realistic, feasible, based on plausible scenarios and reasonable assumptions and shall have a planned implementation schedule compatible with the exit and termination terms established in the relevant contractual arrangements. Also, ensure smooth exit and workload migration to another service provider without business disruption, compliance loss, or service quality decline.	
Third-party Risk Management	17	Third-party Risk Management	17.6	Annual Reporting of New Arrangements	Report new service provider arrangements to the regulator, especially those supporting critical or important functions, to the regulator on a yearly basis, with immediate notification for critical services.	

TPRM.18 Subcontracting Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Third-party Risk Management	18	Subcontracting Management	18.1	Third-Party Subcontractor Due Diligence	Implement due diligence procedures to evaluate third-party ICT service providers' subcontracting practices. Ensure these providers actively engage in operational reporting and testing, demonstrating their ability to assess subcontractor capabilities effectively. Require active involvement and notification of the financial entity in subcontracting decisions, ensuring alignment with contractual arrangements. Verify that subcontracting agreements reflect the terms and conditions outlined in the primary contract between the financial entity and the third-party provider. Assess the third-party provider's organizational structure, resources, and information security standards, including incident response and risk management mechanisms. Mitigate risks associated with subcontractor failure and geographical location, considering potential impacts on digital operational resilience and financial stability. Address any barriers to audit and access rights for competent authorities and the financial institution.	1.1 (RTS SCM) 2.1 (RTS SCM) 3.1 (RTS SCM) 3.2 (RTS SCM) 3.3 (RTS SCM) 5.1 (RTS SCM) 5.2 (RTS SCM) 5.3 (RTS SCM) 5.4 (RTS SCM) 6.1 (RTS SCM) 6.2 (RTS SCM) 6.3 (RTS SCM) 6.4 (RTS SCM)
Third-party Risk Management	18	Subcontracting Management	18.1	Subcontracting Risk Management	Establish a risk management process to oversee subcontracting activities effectively. Monitor the entire ICT subcontracting chain, documenting conditions and ensuring compliance with contractual obligations and the obligation to maintain and update the register of information. Review contractual documentation and key performance indicators to verify adherence to established conditions throughout the subcontracting chain. Require advance notice of significant changes to subcontracting arrangements, enabling thorough risk assessment and mitigation. Ensure that the right to approve changes or request modifications to material subcontracting activities is added to the contracts with the third-party ICT service providers that provide critical or important functions. Implement proactive measures to address identified risks and enhance subcontracting oversight.	
Third-party Risk Management	18	Subcontracting Management	18.1	Subcontracting Monitoring	Institute a process of continuous improvement and monitoring to enhance subcontracting practices and mitigate associated risks. Regularly review and update subcontracting conditions based on changing business environments and risk assessments. Conduct periodic assessments of subcontracting criteria, including ICT threats, concentration risks, and geopolitical factors. Ensure uniform implementation of subcontracting conditions across all subsidiaries, within permissible limits. Monitor and evaluate the effectiveness of subcontracting controls through independent reviews and compliance audits. Proactively identify and address any deficiencies or emerging risks to strengthen subcontracting governance and oversight.	

Resilience testing

RT.19 Digital Operational Resilience Testing

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Resilience testing	19	Digital Operational Resilience Testing	19.1	Resilience Testing Program	Establish a risk-based digital operational resilience testing program encompassing identification, classification, and full remediation of test deficiencies based on risk landscape and criticality of assets and services. Utilize independent internal or external parties for conducting tests, ensuring clear Segregation of Duties (SoD). Conduct yearly tests on all systems and applications supporting critical or important functions (see controls 19-20 for the digital operational resilience tests).	24.1 24.2 24.3 24.4 24.5 24.6 25.1
Resilience testing	19	Digital Operational Resilience Testing	19.2	Diverse Testing Modalities	Employ a range of tests including vulnerability assessments, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires, scanning software solutions, source code reviews (where applicable), scenario-based tests, compatibility testing, performance testing, end-to-end testing, and penetration testing as appropriate.	

RT.20 Threat-led Penetration Testing (TLPT)

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Resilience testing	20	Threat-led Penetration Testing (TLPT)	19.3	Periodic TLPT Testing	Conduct Threat-led penetration testing (TLPT) every three years, aligning with the entity's risk profile. Ensure TLPT covers all critical or important functions and test on live production systems. Provide the regulator with a report encompassing TLPT findings, remediation plans, and documentation demonstrating adherence to this control. Perform TLPT according to the DORA TLPT framework (based on the TIBER-EU framework) as defined in the corresponding RTS. *Note that this control is only applicable for financial institutions wich are eligible for TLPT. Refer to the RTS on TLPT for more information on applicability.	26.1 26.2 26.3 26.5 26.6 26.8 27.1 27.2 2 (RTS TLPT) 3 (RTS TLPT) 4 (RTS TLPT) 5 (RTS TLPT) 6 (RTS TLPT) 7 (RTS TLPT) 8 (RTS TLPT) 9 (RTS TLPT) 10 (RTS TLPT) 11 (RTS TLPT) 12 (RTS TLPT) 13 (RTS TLPT)
Resilience testing	20	Threat-led Penetration Testing (TLPT)	20.1	Outsourced System testing	Extend TLPT to critical outsourced systems, processes, and technologies. The entity shall remain responsible for control compliance. Collaborate with the service providers to establish risk management controls, mitigating risks to data, assets, and critical functions. *Note that this control is only applicable for financial institutions wich are eligible for TLPT. Refer to the RTS on TLPT for more information on applicability.	
Resilience testing	20	Threat-led Penetration Testing (TLPT)	20.2	Selection of TLPT Testers	Engage either internal or external TLPT testers, with external testers contracted every third TLPT cycle. Ensure internal testers are regulator-approved, possess adequate resources, and engage external threat intelligence providers. Select TLPT testers based on reputation, expertise in threat intelligence, penetration testing, and red team practices, relevant certifications, independent assurance, and indemnity insurance coverage. *Note that this control is only applicable for financial institutions wich are eligible for TLPT. Refer to the RTS on TLPT for more information on applicability.	

Security Management

SM.21 Architectural and Network Security

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Security Management	21	**Architectural and Network Security**	21.1	**Network Design and Segmentation**	Design the network infrastructure in a way that allows it to be instantaneously severed or segmented to minimize and prevent contagion. Have provisions for temporarily isolating subnetworks and network components/devices. Ensure redundant capabilities are equipped with sufficient resources, capabilities, and functions (e.g., redundant network setup). Systems and networks must be segregated based on function criticality, classification, and overall risk profile. Maintain a separate network for asset administration. Provide a Layer 3 or 7 (L3/L7) visual representation of all networks and data flows. Conduct yearly performance reviews of the network architecture/design.	9.4 (b) 12.4 13.1 (RTS RM) 13.2 (RTS RM)
Security Management	21	**Architectural and Network Security**	21.2	**Network Security**	Implement controls to prevent and detect unauthorized network connections. Establish and maintain a secure configuration baseline for all network components, following vendor instructions, industry standards, and best practices. Ensure Confidentiality, Integrity, and Availability (CIA) of data during network transmission. Prevent and detect data leakage, and secure data transfer with external parties. Implement measures to secure network traffic between internal networks and the internet/external connections. Apply encryption for all communication protocols over corporate, public, domestic, thirdparty, and wireless networks, based on data classification and risk assessments. Regularly review roles and responsibilities for defining, implementing, approving, changing, and reviewing firewall rules and connection filters. Financial entities shall perform the review of firewall rules and connections filters on a regular basis according to the classification and overall risk profile of ICT systems involved. For the ICT systems supporting critical or important functions, the financial entities shall verify the adequacy of the existing firewall rules and connection filters at least every six months.	
Security Management	21	**Architectural and Network Security**	21.3	**Session Management**	Enforce procedures to limit, lock, and terminate system and remote sessions after a predefined period of inactivity.	

SM.22 Security Monitoring & Log Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Security Management	22	**Security Monitoring & Log Management**	22.1	**Security Monitoring (SIEM)**	Put in place mechanisms to detect anomalous activities, including network performance issues, incidents (reported by the third-parties in the services that they provide), and potential material single points of failure. The mechanisms shall enable multi-layers of control, define alerting thresholds, monitoring on specific events and criteria to automatically trigger incident response. Identify and implement tools generating alerts of anomalous activities and behaviour, at least for ICT assets and information assets supporting critical or important functions. Devote sufficient resources to detection and monitoring activities, especially to cybersecurity attacks.	10.1 10.2 10.3 9.1 (RTS RM) 9.2 (RTS RM) 12.1 (RTS RM) 12.2 (RTS RM) 23.2 (RTS RM) 23.3 (RTS RM) 23.4 (RTS RM)
Security Management	22	**Security Monitoring & Log Management**	22.2	**Event Identification for Logging**	Identify events to be logged, covering logical access, physical access, identity management, capacity management, change management, ICT operation (including system activity), and network traffic activities (including network performance). Determine the level of detail for the logs, aligning with the purpose for which the logs were created and to enable effective detection of anomalous activities. Define retention periods for logs, considering business and security objectives, the purpose of recording logs, and risk assessments.	
Security Management	22	**Security Monitoring & Log Management**	22.3	**Secure Handling of Log Data**	Implement measures to secure and handle log data, taking into account the purpose for which the logs were created. Establish measures to detect failures in logging systems. Protect the recording of anomalous activities against tampering and unauthorised access at rest, in use, where relevant, and in transit.	

SM.23 Data and (Legacy) System Security

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Security Management	23	**Data and (Legacy) System Security**	23.1	**ICT (Security) Systems, tools, and solutions**	Design, procure, and implement security solutions and tooling with the goal to ensure resilience, continuity, and CIA of ICT systems, particularly those supporting critical or important functions.	9.2 9.3 11.2 (RTS RM) 20.1 (RTS RM)
Security Management	23	**Data and (Legacy) System Security**	23.2	**Data Protection Practices**	Establish a secure configuration baseline for ICT assets, incorporating industry practices and techniques to minimize exposure to cyber threats. Deploy security measures to ensure CIA, prevent data loss and leakage, and protect against malicious codes. Protect data from risks arising from data management, including poor administration, processing risks, and human error. Ensure secure transfer of data and minimize the risk of data corruption or loss, unauthorized access, and technical flaws that may hinder business activity. Implement access restrictions based on data classification schemes. Regularly verify the effective deployment of these baselines.	
Security Management	23	**Data and (Legacy) System Security**	23.3	**Vendor Recommended Security Settings**	Consider the security measures and settings recommended by the third-party service provider delivering the ICT service. Implement technical and organisational measures to minimise the risks related to the infrastructure used and managed by the ICT third-party service provider.	
Security Management	23	**Data and (Legacy) System Security**	23.4	**Endpoint Devices**	Enforce usage requirements for portable and nonportable endpoint devices. Ensure that only authorized data storage media, systems, and endpoint devices are used to transfer and store data. Implement security measures to ensure that teleworking and the use of private endpoint devices do not adversely impact the overall security of the entity. This includes having a centralized management solution to remotely manage and wipe endpoint devices, security mechanisms that cannot be modified, removed, or bypassed, and the use of removable data storage devices only when the residual ICT risk remains within predefined risk tolerance levels. Enforce security measures to allow only authorized software installation on systems and endpoint devices.	
Security Management	23	**Data and (Legacy) System Security**	23.5	**Secure Data Deletion and Disposal**	Establish a process to securely delete data on and offpremises. Establish a process to securely dispose or decommission data storage devices on and offpremises that contain confidential information.	

SM.24 Encryption and Cryptography

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Security Management	24	Encryption and Cryptography	24.1	Data Encryption	Define rules for encrypting data at rest, in transit, and, where applicable, in use, considering data classification and risk assessments. Specify procedures when encryption of data in use is not feasible, ensuring processing in a separate and protected environment or taking equivalent measures. Implement rules for encrypting internal network connections and traffic with external parties, aligned with data classification and risk assessments.	6.1 (RTS RM) 6.2 (RTS RM) 6.3 (RTS RM) 6.4 (RTS RM) 6.5 (RTS RM)
Security Management	24	Encryption and Cryptography	24.2	Cryptographic Key Management and Lifecycle	Establish protocols for the proper use, protection, and lifecycle management of cryptographic keys. Define criteria for selecting cryptographic techniques and practices, incorporating best practices and industry standards. Employ mitigation and monitoring measures if adherence to these practices and standards is not possible. Outline requirements for managing and controlling cryptographic keys throughout their lifecycle, including generation, storage, backup, archiving, retrieval, transmission, retirement, revocation, and destruction. Establish methods to recover cryptographic keys in case of loss, compromise, or damage. Monitor crypto-analysis developments and, when necessary, update or change cryptographic technology. Implement mitigation and monitoring measures if changing or updating the cryptographic technology is not feasible. Maintain a register for all certificates and certificate storing devices.	7.1 (RTS RM) 7.2 (RTS RM) 7.3 (RTS RM) 7.4 (RTS RM) 7.5 (RTS RM)

SM.25 Identity and Access Management

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Security Management	25	Identity and Access Management	25.1	Identity Management	Assign a unique identity to each staff member or staff of the third-party service provider accessing information and ICT assets. Implement a lifecycle management process for identities, covering creation, change, recertification, temporary deactivation, and termination of user accounts. Utilize automated solutions where applicable.	20.1 (RTS RM) 20.2 (RTS RM) 21.1 (RTS RM)
Security Management	25	Identity and Access Management	25.1	Privilige Access Management	Define access rights based on need-to-know, need-to-use, and least privilege principles, including provisions for remote and emergency access. Enforce segregation of duties to prevent unjustified access or combinations that could circumvent controls. Ensure user accountability by limiting generic and shared user accounts, enabling user identification for all ICT system actions. Implement controls and tools to restrict unauthorized access.	
Security Management	25	Identity and Access Management	25.1	Account Management	Establish procedures for granting, changing, and revoking access rights, specifying roles and responsibilities. Define retention periods for access logs. Assign privileged, emergency, and administrator access on a need-to-use or ad-hoc basis, with automated solutions for privilege access management. Withdraw access rights promptly upon termination of employment or when no longer required. Conduct periodic reviews of access rights, ensuring at least annual reviews for non-critical ICT systems and semi-annual reviews for critical systems.	
Security Management	25	Identity and Access Management	25.1	Authentication Methods	Use authentication methods commensurate with the classification and risk profile of ICT assets. Implement strong authentication methods, particularly for remote access, privileged access, and access to critical ICT assets.	

SM.26 Physical and Environmental Security

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Security Management	26	**Physical and Environmental Security**	26.1	**Physical and Environmental Security**	Implement measures to safeguard the environment (premises, data centers, and sensitive designated areas) where important assets are located from attacks, accidents and from environmental threats and hazards. The level of protection from environmental threats should be commensurate with the importance of the asset storage location and the criticality of operations. Safeguard assets both within and outside the entity's premises, ensuring the Confidentiality, Integrity, and Availability (CIA) of these assets. These measures should be determined based on the outcomes of a risk assessment. This also includes practices like maintaining a clean desk and ensuring screens are clear at processing facilities and access to critical ICT assets. Identify and record authorized personnel entering critical locations of the financial entity. Grant physical access rights to critical ICT assets based on need-to-know, least privilege principles, and ad-hoc requirements according to the access management policy. Monitor physical access to premises, data centers, and designated sensitive areas, aligned with asset classification and area criticality. Regularly review and promptly revoke unnecessary physical access rights.	18.1 (RTS RM) 18.2 (RTS RM) 21.1 (RTS RM)

SM.27 Security Awareness

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Security Management	27	**Security Awareness**	27.1	**Resilience Training Programs**	Implement security awareness and digital operational resilience training as integral components of staff training schemes and ensure training extends to all staff members, including senior management. Customize training intensity based on employee roles and functions. For the training content, cover topics such as network security, insights from prior incidents, threat intelligence, defenses against intrusions, data protection measures (e.g., encryption, cryptography). Conduct the resilience training program on an annual basis. Staff shall be informed on the ICT security policies, procedures and protocols and be made aware of the reporting channels put in place for detecting anomalous activities. Upon termination of employment, all staff are required to return all ICT assets and information assets.	5.2 13.6 19.1 (RTS RM)
Security Management	27	**Security Awareness**	27.2	**Inclusion of Third-Party Providers**	Incorporate ICT third-party service providers as participants in relevant training programs, where appropriate. Third-parties shall be informed on the ICT security policies, procedures and protocols and be made aware of the reporting channels put in place for detecting anomalous activities. Upon termination of employment or contract termination, the third-parties are required to return all ICT assets and information assets that belong to the financial entity.	

SM.28 Security Awareness

DORA Domains:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Security Management	28	Vulnerability and Patch Management	28.1	Resource Management	Identify and maintain relevant and trustworthy information resources to build and sustain awareness about vulnerabilities. Track the usage of thirdparty libraries, including open source, by monitoring versions and potential updates (see also 28.2-3).	25.2 10.1 (RTS RM) 10.2 (RTS RM) 10.3 (RTS RM) 10.4 (RTS RM)
Security Management	28	Vulnerability and Patch Management	28.2	Vulnerability Management	Conduct automated vulnerability scanning and assessments on ICT assets. For assets supporting critical or important functions, perform scans and assessments on a weekly basis. Record detected vulnerabilities, monitor their resolution status, and verify the remediation of vulnerabilities. Disclose vulnerabilities responsibly to clients/customers, financial counterparts, and the public when appropriate. Ensure thirdparty service providers report vulnerabilities related to the services they offer. This includes investigating vulnerabilities, determining root causes, and implementing appropriate solutions by the service providers. ***Specific to central securities depositories and central counterparties: perform vulnerability assessments before any deployment or redeployment of new or existing applications and infrastructure components, and ICT services supporting critical or important functions.**	
Security Management	28	Vulnerability and Patch Management	28.3	Patch Management	Identify and evaluate available ICT assets (e.g., software and hardware) patches and updates using automated tools, to the extent possible. Deploy patches to address identified vulnerabilities. Prioritize the deployment of patches and other mitigation measures based on the criticality of the vulnerability and the classification and risk profile of the affected assets. Establish emergency procedures for patching and updating ICT assets. Test and deploy ICT asset patches and updates. Set due dates for the installation of ICT asset patches and updates, and establish escalation procedures in case the due dates cannot be met. In cases where no patches can be applied or are available, identify and implement alternative mitigation measures within the set due dates.	

5 Conclusion

The DORA in control framework offers a crucial tool for organizations aiming to enhance their operational resilience and to comply with multiple regulatory standards.

Our study report underscores the importance of a structured four-step approach to DORA readiness:

1. Assessing the organization's critical and/or important functions. This necessitates a comprehensive overview of all key processes and identifying the ICT infrastructure (including third-parties) that supports and is essential to the operations of these processes.
2. Performing a risk assessment on this ICT infrastructure. The assessment helps establish a risk profile and prioritize areas that require attention.
3. Performing a gap assessment based on the DORA in control framework. Such analysis identifies where the institution currently stands vis-à-vis DORA requirements and highlights areas where improvements are needed.
4. Developing a plan or roadmap, focusing on solutions and mitigating measures to address the identified gaps and root causes and ensure compliance with DORA.

Having performed the above four steps will not only help financial institutions on their journey toward digital operational resilience, but should also prove useful in fulfilling the oversight expectations of supervisory authorities. We have already heard supervisory announcements stating that organizations will be requested to submit gap assessments and roadmaps for compliance.

What's more, applying an engineering's perspective to the DORA in control framework – its construction and its implementation – is essential for addressing the actual root causes of ICT issues rather than merely checking boxes for compliance. By fostering a culture of problem-solving and innovation, we move beyond surface-level fixes toward sustainable solutions that enhance both resilience and efficiency.

Taking the systematic, holistic approach we have outlined, organizations can achieve DORA compliance while also cultivating a proactive framework that enables them to navigate the increasingly complex regulatory landscape. This will also ensure they stay well-equipped to face the future and, in particular, its many ICT challenges and opportunities.

To further support organizations with DORA compliance, the NOREA Dora taskforce plans to continue publishing more guidelines for effective and efficient implementation. For the latest guidelines, please see https://www.norea.nl/dora.