Digital Operational Resilience Act (DORA) Implementation Guidance

Prepared by:

FS-ISAC's DORA Working Group

Digital Operational Resilience Act

Implementation Guidance

Contents

Executive Summary

This FS-ISAC DORA Working Group publication aims to help the financial services sector become compliant with the European Union Parliament's Digital Operational Resilience Act (DORA)[i]. DORA affects the resilience and cybersecurity of many financial services organisations in EU countries, and its requirements are to be applied by each nation's financial services regulators. Financial services organisations' compliance will be required by 17 January 2025.

Part of the EU's Digital Finance Package (DFP)[ii], DORA aims to harmonise digital resilience regulations throughout the EU and "achieve a high level of digital operational resilience for regulated financial entities", according to the Act's preamble.

DORA requirements are not radically different to many other resilience and cyber security regulations and laws, but DORA collates these and raises the bar significantly in some areas. Some requirements are more detailed and specific than many principal-based regulations – and DORA introduces some new requirements, such as those regarding critical third-party providers (CTPPs)[iii].

Any financial services firm, wherever it is headquartered, must comply with DORA in its EU operations and will need to decide whether to implement DORA outside of their EU operations. However, regulators across the world are watching DORA developments closely and will probably implement some aspects of it – the UK Financial Services and Markets Act 2023[iv], for example, covers critical third-party providers similarly to DORA (Article 31).

It would be a great mistake to assume that being compliant with other regulations will ensure that a firm is compliant with DORA. We recommend that financial services organisations fully assess their operations in light of DORA regulations.

Background

DORA, the EU Digital Operational Resilience Act, is an EU law which affects all countries in the European Union. It forms part of the EU's Digital Finance Package (DFP) and aims to harmonise digital resilience regulations throughout the EU, so all EU countries will have the same requirements that will be applied by their Financial Services (FS) regulators. It also aims "to achieve a high level of digital operational resilience for regulated financial entities" (Recital 105 preamble). Institutions can no longer just defend themselves; they must adopt a posture that assists in maintaining the reliability and integrity of financial services in the case of disruptions, incidents, attacks, etc.

Any financial services firm, wherever they are headquartered, will need to comply with DORA in their operations in the EU and will need to decide whether they implement DORA for their EU operations solely or more widely. Over time DORA is likely to have a major impact not just in the EU, but on resilience in FS globally. Regulators in other countries are watching DORA developments closely and are likely to implement some of the more novel aspects of DORA in the future. For example, chapter 2 of the recent UK Financial Services and Markets Act 2023 covers 'Critical Third-Party Providers', which is also a key requirement of DORA (Article 31).

One question frequently asked is: How different is DORA to other resilience and cybersecurity regulations? While DORA is not radically different, it brings together many requirements under one common banner and raises the bar in some areas. It also introduces new requirements, such as those for Critical Third-Party Providers (CTPPs), and is more detailed and specific than many other regulations that are often more principal based. It would be a great mistake to assume that being compliant with other regulations will ensure that one is compliant with DORA. We recommend that a full assessment is made.

DORA Timescales

The first batch of DORA standards have been finalized. Some of the standards in the second batch are still being drafted and finalized, and will be complete on 17 July 2024. Implementing both batches may take financial services firms extensive effort and time. Consequently, we recommend that any financial services institution with operations in the EU start a DORA implementation project without delay, if they haven't done so already.

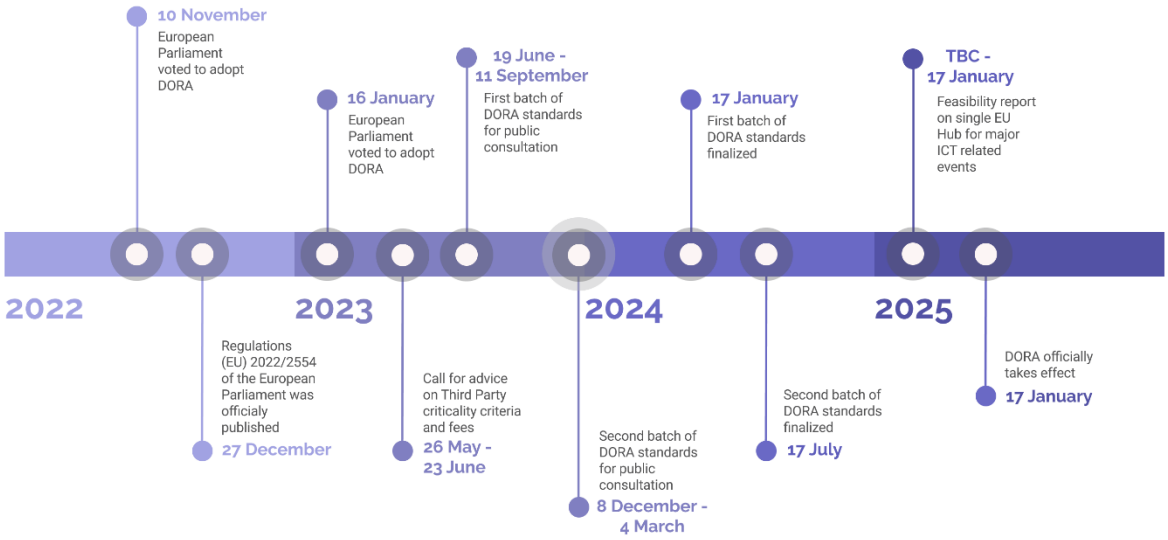

Figure 1. DORA timeline from 10 November 2022 to 17 January 2025

Scope of DORA – Who Needs to Comply

DORA applies to many types of financial services firms, but not all. For example, it does not apply to 'small or medium-sized enterprises'. In general, the following types are in scope of DORA (See DORA Article 2 for the complete list):

- Credit and payment institutions
- Account information service providers
- Electronic money institutions
- Investment firms
- Cryptocurrency asset service providers

- Central securities depositories
- Central counterparties
- Trading venues and trade repositories
- Managers of alternative investment funds
- Management companies
- Data reporting service providers
- Insurance and reinsurance undertakings and intermediaries
- Institutions for occupational retirement provision
- Credit rating agencies
- Administrators of critical benchmarks
- Crowdfunding service providers
- Securitisation repositories
- Information and communication technology (ICT) third-party service providers

The Five Pillars of DORA

There are five essential elements of DORA, with some being far more extensive than others. Some of these are complete, but others contain additional details in the DORA standards, the Regulatory Technical Standards (RTS), Implementing Technical Standards (ITS) and guidelines. See Appendix 1 for a full list and relevant DORA articles.

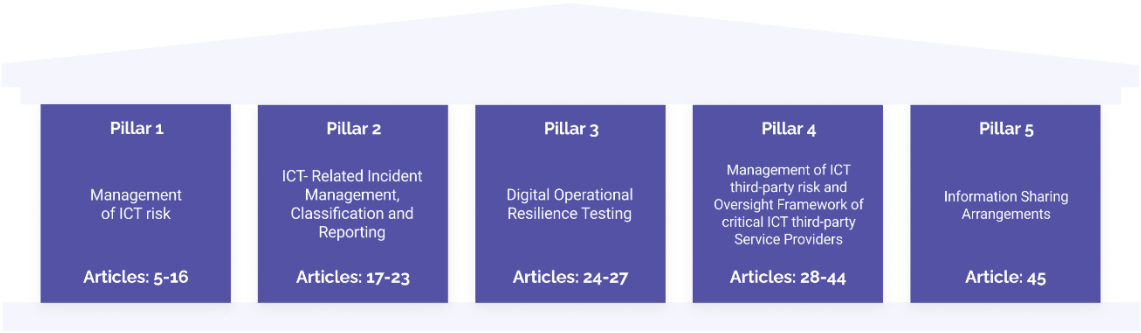

Figure 2. The Five Pillars of DORA

ICT risk management (articles 5-16)

- Governance and organisation

- ICT risk management framework
- ICT systems, protocols, and tools
- Identification
- Protection and prevention
- Detection; Response and recovery
- Backup policies and procedures, restoration and recovery procedures and methods
- Learning and evolving
- Communication
- Further harmonisation of ICT risk management tools, methods, processes, and policies
- Simplified ICT risk management framework

ICT-related incident management, classification, and reporting (articles 17-23)

- ICT-related incident management process
- Classification of ICT-related incidents and cyber threats
- Reporting of major ICT-related incidents and voluntary notification of significant cyber threats
- Harmonisation of reporting content and templates
- Centralisation of reporting of major ICT-related incidents
- Supervisory feedback; Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions

Digital operational resilience testing (articles 24-27)

- General requirements for the performance of digital operational resilience testing
- Testing of ICT tools and systems
- Advanced testing of ICT tools, systems, and processes based on TLPT
- Requirements for testers for the carrying out of TLPT

Management of ICT third-party risk and Oversight Framework of critical ICT third-party service providers (articles 28-44)

- General principles
- Preliminary assessment of ICT concentration risk at entity level
- Key contractual provisions

- Designation of critical ICT third-party service providers
- Structure of the Oversight Framework
- Tasks of the Lead Overseer; Operational coordination between Lead Overseers
- Powers of the Lead Overseer
- Exercise of the powers of the Lead Overseer outside the European Union
- Request for information
- General investigations; Inspections
- Ongoing oversight
- Harmonisation of conditions enabling the conduct of the oversight activities
- Follow-up by competent authorities
- Oversight fees
- International cooperation

Information sharing arrangements (article 45)

- Information sharing arrangements on cyber threat information and intelligence

DORA Standards

In addition to the main articles in DORA, the Regulatory Technical Standards, and Implementing Technical Standards and guidelines, add additional requirements. These are aimed at harmonisation and facilitating implementation. There are two main publication batches of the standards, as well as additional consultation papers. These are shown below with their draft and final publication dates and, the DORA articles they relate to:

First batch of standards: 19 June 23 – 17 January 2024

- ICT Risk management framework (RTS: article 15)
- Simplified ICT risk management framework (RTS: article 16)
- Criteria for the classification of ICT-related incidents (RTS: article 18)
- Templates to register information (ITS: article 28)
- Policy on ICT services performed by a third party (RTS: article 28)

Second batch of standards: 8 December 23 – 17 July 2024

- Reporting of major ICT-related incidents (RTS: article 20)
- Reporting details for major ICT-related incidents (ITS: article 20)
- Guidelines on the estimation of aggregated costs/losses caused by major ICT-related incidents (Article 11)

- Threat led penetration aspects (RTS: article 26)
- Elements when sub-contracting critical or important functions (RTS: article 30)
- Cooperation between European Supervisory Authorities (ESAs) and competent authorities (CAs) regarding the structure of the oversight (GL: article 32)
- Information on oversight conduct (RTS: article 41)

Additional consultation papers

- Advice on criticality criteria and fees (26 May – 30 September 2023; article 43)
- Feasibility report on single EU hub for major ICT-related events (tbc – 17 January 2025: article 21)

When assessing compliance with DORA, the main articles should be read in conjunction with any related DORA standards as shown above. For example, Article 15 on Risk Management should be read in conjunction with the RTS 'ICT Risk management framework'.

Key Steps to Consider in a DORA Project

The form of a DORA project and its stages, milestones, and timescales depends on the type, size, and geographic spread of the organisation. It will also depend on the divisions or parts that will be impacted.

The following is a high-level guide to some of the steps financial services firms should consider. Some of these steps might run in parallel.

Step	Details
1. Conduct initial review of DORA	• Review DORA and determine the likely project size. • Involve senior management and get their buy-in.
2. Establish Dora project team	• Decide which groups and specialists should be involved and provide input. • Consider the personnel to be included and the extent of their likely involvement.
3. Conduct detailed review of DORA and its standards	• Specialists conduct detailed review. • Identify DORA's impact on relevant policies.

4. Map current state against DORA	• Create detailed mapping matrix of DORA and its standards against policies. Consider existing ICT resilience and cyber strategy, management plans, policies, procedures, and operations. Many aspects of DORA may already be covered by a number of teams and their respective policies and procedures. • Score current level of compliance and create RAG status. • Identify gaps, areas of non-compliance and areas of partial compliance.
5. Conduct options analysis	• Consider options for addressing gaps and weaknesses, considering costs, implementation, risks etc. • Consider policy and procedure changes required. • Design the geographic and system scope of remedial action to meet DORA requirements, determining whether compliance will relate only to EU operations, or include some or all non-EU operations. • Obtain senior management's agreement on options.
6. Create project plan	• Determine subprojects. • Decide on milestones. • Include some flexibility to allow for changes directed by the second batch of DORA standards which will be finalised June 2024. • Get final approval.
7. Implement plan and complete DORA project	• Run DORA project, which should be complete before or on 17 January 2025. • Evaluate project successes and lessons learned.

Figure 3. Key steps in a DORA project

1. Conduct initial review of DORA

- Review DORA and determine the likely project scope.
- Involve senior management and get their buy-in.

In many organisations, a good first step towards DORA would be for an individual or a small group from compliance, risk management, resilience, and/or cybersecurity functions to review the Act. Their objective should be to get an idea of the size of the project, potential challenges, and necessary personnel.

Senior management should also be engaged from an early stage and then they should drive the whole DORA project.

2. Establish DORA project team

- Decide which groups and specialists should be involved and provide input.
- Consider the personnel to be included and the extent of their likely involvement.
- Appoint a dedicated project/programme manager.

DORA's scope is extensive and includes different domains concerning resilience, risk, security, and third-party management and procurement. DORA brings all these together under one regulation. Consequently, a DORA implementation and compliance project should ideally include representation from all such teams. In some cases, they may not all form the main team, but they should be engaged and provide input. The make-up of the teams that should be involved will depend on the structure and scope of the organisation. Consider which should be included and the extent of their likely involvement. Subject matter experts will need to be engaged for certain topics, i.e. Incident management and threat-led penetration testing.

In many cases a dedicated project/programme manager should also be appointed. DORA involves many different functions so the manager may need to have some degree of independence, possibly coming from a central PMO function.

As a general guide, the following functions may be affected and should provide input:

- Resilience/business continuity
- Third-party and supply chain management
- Cybersecurity
- Risk management
- Threat and vulnerability management
- Incident management and reporting
- Security testing and red/blue teams
- Scenario exercising
- Legal
- Policy
- Compliance
- ICT

3. Conduct detailed review of DORA and its standards

- Specialists conduct detailed review.
- Identify DORA's impact on relevant policies.

Specialists should conduct a detailed review of DORA requirements and the current state of the standards. That review should identify DORA's impact on organisational policies, identify gaps, and note potential implementation or operational difficulties.

4. Map current state against DORA

- Create detailed mapping matrix of DORA and its standards against policies. Consider existing ICT resilience and cyber strategy, management plans, policies, procedures, and operations. Many aspects of DORA may already be covered by a number of teams and their respective policies and procedures.
- Score current level of compliance and create RAG status.
- Identify gaps, areas of non-compliance, and areas of partial compliance.

A detailed mapping exercise should be conducted that includes all existing policies, standards, procedures, and operations. Some financial services firms may find that their strategy and management plans will need to be changed as well. Many aspects of DORA may already be in operation and require no further action.

Some organisations will have a map against existing regulations. In these cases, DORA can just be added to the map. Where this does not already exist, such a map should be considered for the future. Many other regulations overlap with DORA.

The current level of compliance with DORA requirements should also be assessed and a RAG status created. This should identify areas of compliance, areas of partial compliance, and gaps. It may also be necessary to flag some areas for further investigation where additional input is required, either from internal or external specialists.

5. Conduct options analysis

- Consider options for addressing gaps and weaknesses, considering costs, implementation, risks, etc.
- Consider policy and procedural changes required.

- Decide the geographic and system scope of remedial action to meet DORA requirements. For example, determining whether compliance will relate only to EU operations or include some or all non-EU operations.
- Obtain senior management's agreement on options.

Options to address weaknesses and gaps with DORA should now be assessed. There may only be one viable option, or there may be several. Consider costs, resources, potential timescales, implementation challenges, and risks. Take account of the policy and procedural changes required, now and in the future.

Another important factor is the geographic and system scope of remedial action that will be required. This can be a complex decision. However, while determining which non-EU operations will comply with DORA, financial services organisations may find it advantageous to comply with DORA outside the EU. In some cases, DORA compliance may offer better resilience or simpler operations. For some organisations, compliance may prove necessary, such as those with a technology system shared by operations both within and outside the EU.

Senior management should be involved in the analysis and decide the best options.

6. Create project plan

- Determine subprojects.
- Decide on milestones.
- Include some flexibility to allow for changes directed by the second batch of DORA standards, which will be finalized July 2024.
- Get final approval.

Create a detailed project plan and roadmap that addresses weaknesses and gaps, subprojects, milestones, timescales, resources, and costs. The scale of the project will depend on the size and structure of the organization, how well its policies and procedures already align with DORA, and the maturity of its resilience, risk, and cybersecurity programs. The plan should enable full compliance on or before 17 January 2025, when compliance with DORA is required.

Build some flexibility into the plan to allow for changes introduced in the second batch of DORA standards, which will be finalized in July 2024.

Senior management should agree to the project's costs and resource requirements and approve the plan. Depending on the size of the project and the organization's structure, the plan may require approval from technology leaders, all or some executives, and/or the full board.

7. Implement plan and complete DORA project

- Run DORA project, which should be complete before or on 17 January 2025.
- Evaluate project successes and lessons learned.

Once the project has been fully approved and supported, begin implementation. Track progress and forward reports to senior management. Flag delays or difficulties so that they can be addressed without delay -- for many firms, timescales may be tight.

Compliance with DORA will be required on 17 January 2025. If, at that time, there are areas in which the company has not fully met DORA requirements, an action plan to address these may be required. Regulators may need to be consulted.

There also needs to be a hand-over process to any new teams formed and any new or amended processes in a transition to normal business operations. Lastly, it is good practice to evaluate project successes, problems, and lessons learned. This record may help with future compliance projects and any new releases of DORA.

Challenges of DORA

DORA covers many familiar issues, but also introduces some new elements, raises certain standards, and contains more detailed requirements. As such, members of the FS-ISAC DORA Working Group have identified particular challenges relating to implementation. As with any complex regulation or law it is important to review and understand the details.

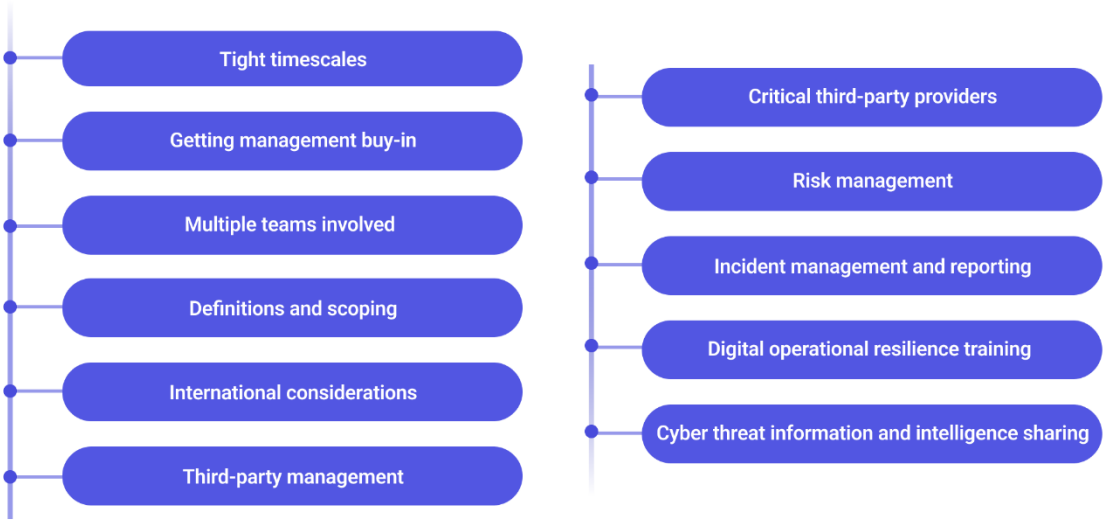

Figure 4. Challenges associated with implementing DORA compliance project

Tight timescales

One of the most challenging aspects of the regulation are the tight timescales necessary to implement DORA. DORA itself was officially published on 27 December 2022 and entered into force on 16 January 2023. However, a significant amount of the details regarding DORA standards have not yet been finalized. FS-ISAC members have noted that the gap analysis against the RTS documents is particularly challenging, as it includes program, policy, and procedure level elements.

Draft copies of the first batch were circulated for public consultation in June 2023 but weren't finalised until January 2024. A second batch of draft standards were published on 8 December 2023 and are now open to public consultation. These won't be finalised until 17 July 2024, but will then need to be translated into the 27 EU languages and submitted to the commission for approval. Firms will then have six months to comply before 17 January 2025. Such timescales are extremely tight, so it is recommended that any financial organisations that will be affected by DORA start working on a compliance project as soon as possible, rather than waiting for all the standards to be completed.

Getting management buy-in

DORA's potential impact on risk, resilience, and security management is very high. Financial services institutions may need to change aspects of their strategies, policies,

and management, which will create additional processes and costs. It is therefore vital to get full senior management buy-in from the start. Some DORA Working Group members have reported they have found this particularly difficult as some DORA standards have not been finalised. One is effectively trying to hit a moving target.

Multiple teams involved

DORA introduces increased complexity and requires close cross-team collaboration. Many DORA requirements cut across teams and functions, such as resilience/business continuity, cybersecurity, risk management, third-party and supply chain management, threat and vulnerability management, incident management and reporting, resilience and security testing, scenario exercising, and regulatory compliance. As a result, analyzing compliance and checking for gaps is challenging, particularly in large firms.

Definitions and scoping

Article 3 of DORA covers definitions. However, several FS-ISAC DORA Working Group members have raised concerns that some of these definitions are vague and are open to interpretation. This requires firms implementing DORA to state precisely how they are interpreting the definitions and to scope work accordingly.

A good example is the definition of a 'critical or important' function which is used repeatedly in DORA. This is defined in Article 3.22 as:

"'Critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective, or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law".

Other terms causing concern include the definition of an ICT service (see Article 3.21), an information asset (Article 3.6), and an ICT asset (Article 3.7). We recommend members take a position and state clearly how they are interpreting these terms, saying what is in or out of scope in their environment. Action is far preferable to inaction.

International considerations

International financial firms with operations both inside and outside the EU may find it a challenge to determine the applicability of DORA to their overseas operations. EU-

headquartered organizations may choose to implement DORA requirements outside the EU, though they will nonetheless remain accountable to local regulations. Similarly, organisations based outside the EU may decide to implement some DORA requirements outside their EU operations, such as those using an ICT system that serves multiple countries.

A key aim of DORA is to harmonise regulations throughout the European Union, and it applies equally in every EU country. However, DORA permits individual member states and their competent authorities, the regulators, the power to impose measures, penalties, and fines for non-compliance (see Article 50.4). National differences over the enforcement of DORA may arise.

Third-party management

A key requirement of DORA is the management of third-party providers, covered in Articles 28 to 44. While resilience and security checks are now a standard part of third-party provider management, DORA significantly raises the bar. This is arguably the most radical part of DORA and has significant implications, particularly for firms with hundreds or even thousands of third-party providers.

Specifically, DORA introduces a requirement to assess concentration risk (Article 28.4 and 29.1), and for ICT services supporting critical or important functions to consider substitution of providers and multiple contracts. This may be especially difficult when a third-party contract is not local but international, or even global. Detailed contract requirements are also required, so many contracts will need to be assessed, renegotiated and updated, which will take time and resources (see Article 30 and the RTS 'Elements when sub-contracting critical or important functions', which won't be finalized until July 2024). Contracts must also include exit strategies (Article 28.8) for ICT services supporting critical or important functions, to ensure contracts can be exited without any disruption.

Another area of concern is the oversight of subcontracting. This potentially moves beyond third parties to fourth, fifth, and nth parties, if the contract underpins a critical or important function (Article 29.2).

Critical third-party providers

DORA includes a new aspect in the regulation of financial services: specific regulation for critical ICT third-party service providers (Articles 31-44). The ESAs are required to

assess and designate the ICT third-party providers deemed critical using criteria specified in Article 31. ESAs will use 11 quantitative and qualitative indicators, along with the necessary information to draft and interpret such indicators, following a two-step approach. Providers designated as critical will be directly regulated by the financial regulators. Over time, this is likely to increase costs and affect the financial provider market. However, significantly, regulation of critical ICT third-party providers will not reduce financial organizations' obligation to manage and oversee the resilience and security of such providers themselves.

Risk management

A sound ICT risk management framework is a key pillar of DORA (see Articles 5-16). The framework should be comprehensive, consisting of several requirements regarding the management of digital risks according to a set risk profile (see RTS on ICT Risk management framework and Simplified ICT risk management framework). The risk management framework described in DORA sets high requirements on both the content of the framework as well as the processes of identification, protection and prevention, detection, and response and recovery of risk. In that way, it is similar to the NIST framework in the United States. Organisations may find it a challenge to integrate these requirements into their existing risk framework.

Incident management and reporting

DORA requires financial organisations to classify and give detailed reports on major ICT-related incidents to a competent authority, namely the local FSA (see Articles 17-23). Competent authorities will therefore have a more prominent role in surveilling how financial institutions manage incidents. DORA standards contain detailed requirements, and work is likely to be needed to integrate these with existing incident processes and systems, Criteria for the classification of ICT-related incidents, Reporting of major ICT-related incidents, Reporting details for major ICT-related incidents, and Guidelines on the estimation of aggregated costs/losses caused by major ICT-related incidents. As part of this, organisations are required to conduct a timely root cause analysis and forward reports to regulators. Some FS-ISAC DORA Working Group members have noted concerns, as it is not known how widely these incident reports might be shared and how secure they will be.

However, a centralized EU hub may be created for reporting major ICT-related incidents. The ESAs have been given the task of preparing a report, due in January 2025, on the feasibility of a central hub.

Digital operational resilience testing

DORA requires the establishment of a digital operational resilience testing program appropriate to the scale and complexity of the business (Articles 24-27). A wide range of tests are required (including scenario-based tests), many of which firms may already have in place, but DORA requires increased focus on the types of tests to perform and how to perform them. Notably larger financial services institutions are generally required to perform threat-based penetration testing by independent accredited parties, potentially including ICT third-party providers. However, there are exceptions for some types of institutions such as small and non-interconnected investment firms. It is therefore important to understand the category of the firm under DORA to determine applicable requirements.

In general, appropriate tests are required at least annually on all ICT systems and applications supporting critical or important functions, and they must be undertaken by independent parties, whether internal or external. Regular testing is required to gain a strategic perspective, which doesn't always exist as tests are often managed in silos (vulnerability testing, penetration testing, business continuity testing, scenario testing etc.). All issues found need to be prioritised, classified, and remediated.

Cyber threat information and intelligence sharing

A key pillar of DORA concerns threat information and intelligence sharing (Article 45). This will be familiar territory for FS-ISAC members. While this is currently voluntary, we understand sharing will likely become mandatory in the future. FS-ISAC is the only intelligence sharing community with a secure platform solely focused on financial services.

The FS-ISAC DORA Working Group

At FS-ISAC, we have seen a large and growing interest in DORA. We started a working group on DORA at the start of 2023 which has proved very popular. Our many members exchange ideas and they are addressing DORA and its challenges. Working group meetings also include knowledgeable external speakers. If an FS-ISAC member firm wishes to join the DORA Working Group, please send an email to FS-ISAC Member Services at memberquestions@fsisac.com.

Appendix 1: Key Articles of DORA

- ICT risk management (articles 5-16)
  - Governance and organisation (article 5)
  - ICT risk management framework (article 6)
  - ICT systems, protocols and tools (article 7)
  - Identification (article 8)
  - Protection and prevention (article 9)
  - Detection (article 10)
  - Response and recovery (article 11)
  - Backup policies and procedures, restoration and recovery procedures and methods (article 12)
  - Learning and evolving (article 13)
  - Communication (article 14)
  - Further harmonisation of ICT risk management tools, methods, processes and policies (article 15)
  - Simplified ICT risk management framework (article 16)
- ICT-related incident management, classification and reporting (articles 17-23)
  - ICT-related incident management process (article 17)
  - Classification of ICT-related incidents and cyber threats (article 18)
  - Reporting of major ICT-related incidents and voluntary notification of significant cyber threats (article 19)
  - Harmonisation of reporting content and templates (article 20)
  - Centralisation of reporting of major ICT-related incidents (article 21)
  - Supervisory feedback (article 22)
  - Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions (article 23)
- Digital operational resilience testing (articles 24-27)
  - General requirements for the performance of digital operational resilience testing (article 24)
  - Testing of ICT tools and systems (article 25)
  - Advanced testing of ICT tools, systems and processes based on TLPT (article 26)
  - Requirements for testers for the carrying out of TLPT (article 27)
- Management of ICT third-party risk and Oversight Framework of critical ICT third-party service providers (articles 28-44)
  - General principles (article 28)
  - Preliminary assessment of ICT concentration risk at entity level (article 29)

- Key contractual provisions (article 30)
- Designation of critical ICT third-party service providers (article 31)
- Structure of the Oversight Framework (article 32)
- Tasks of the Lead Overseer (article 33)
- Operational coordination between Lead Overseers (article 34)
- Powers of the Lead Overseer (article 35)
- Exercise of the powers of the Lead Overseer outside the Union (article 36)
- Request for information (article 37)
- General investigations (article 38)
- Inspections (article 39)
- Ongoing oversight (article 40)
- Harmonisation of conditions enabling the conduct of the oversight activities (article 41)
- Follow-up by competent authorities (article 42)
- Oversight fees (article 43)
- International cooperation (article 44)

- Information sharing arrangements (article 45)
  - Information sharing arrangements on cyber threat information and intelligence (article 45)

Appendix 2: Glossary

In addition to the glossary below, see the Definitions provided in DORA Article 3.

Term	Definition
Competent authority	EU competent authority: any authority appointed in an EU or an European Economic Area (EEA) Member State in accordance with Article 44 of the AIFMD for the supervision of Managers, delegates, depositaries and, where applicable, Covered Funds, or a European territory for whose external relations a Member State is responsible in accordance with Article 355 (3) of the Treaty on the Functioning of the European Union.
DORA	The EU Digital Operational Resilience Act.

ECB	European Central Bank (ECB) which is the central bank of the European Union countries which have adopted the euro.
ESAs	The European Supervisory Authorities (ESAs) are three regulatory agencies established by the EU in 2010, to help facilitate the development and convergence of financial services regulation and supervision across the EU. The three agencies are: ▶ European Banking Authority (EBA) ▶ European Insurance and Occupational Pensions Authority (EIOPA) ▶ European Securities and Markets Authority (ESMA)
ICT services	ICT services under DORA are: digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.
ITS	Implementing Technical Standards (ITS) establishes templates for the register of information.
NIST framework	NIST is the National Institute of Standards and Technology at the US Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data.
RTS	Regulatory Technical Standards (RTS) is a type of regulatory instrument used in the European Union to provide detailed technical specifications for the implementation of certain aspects of DORA legislation.

[i] Regulation - 2022/2554 - EN - DORA - EUR-Lex (europa.eu)
[ii] EUR-Lex - 52020PC0595 - EN - EUR-Lex (europa.eu)
[iii] Regulation - 2022/2554 - EN - DORA - EUR-Lex (europa.eu)
[iv] Financial Services and Markets Act 2023 (legislation.gov.uk)

