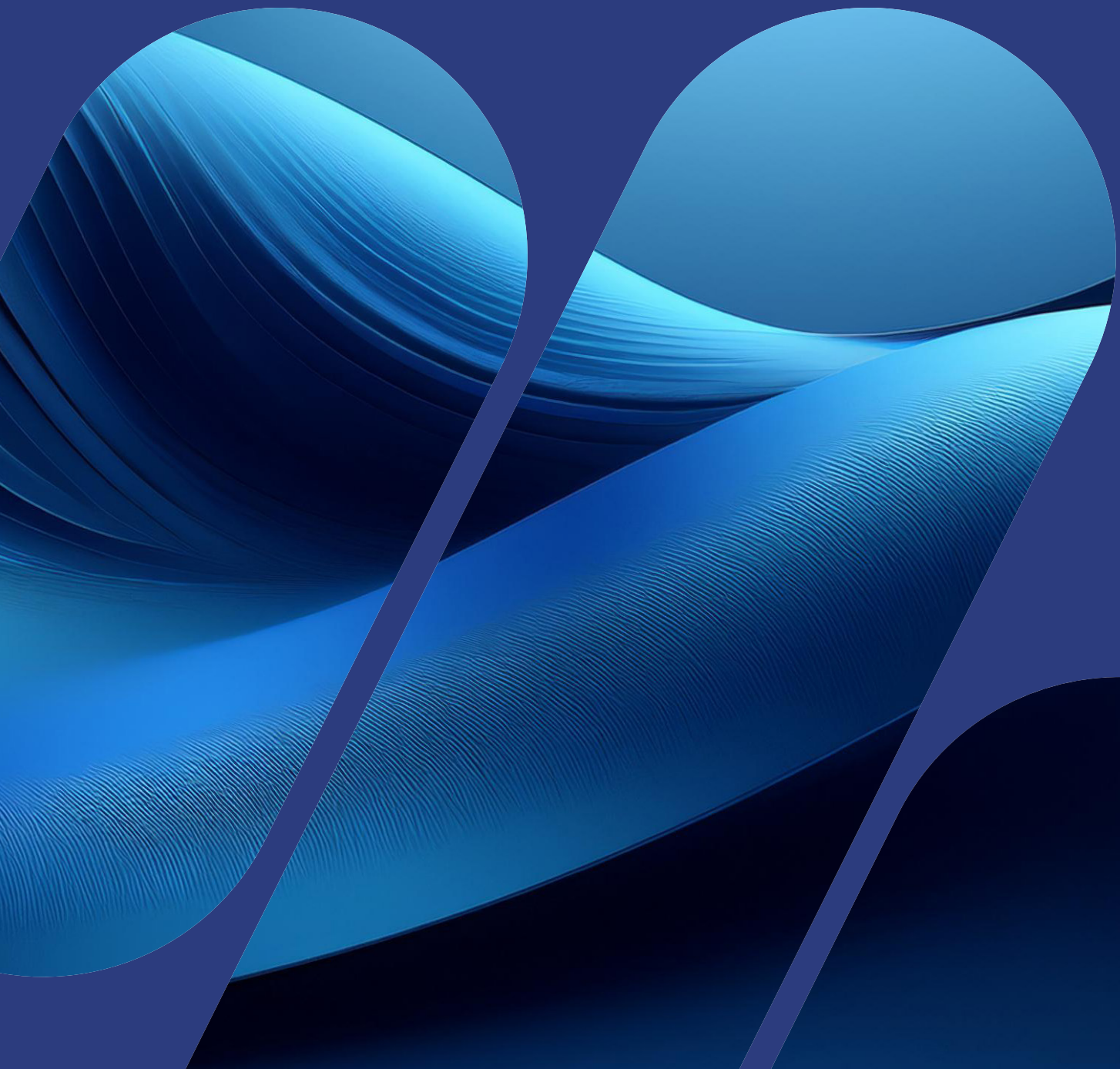
APEX

Digital Operations Resilience Act



Contents

Digital Operations Resilience Act

Introduction

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ('DORA') was published in the Official Journal of the European Union on 27 December 2022. DORA aimed to consolidate and upgrade ICT risk requirements as part of the operational risk requirements which at that point had been addressed separately in various legislative acts of the European Union. DORA forms parts of a larger digital financial package which aims at developing a European approach fostering technological development and ensuring financial stability and consumer protection. This package, originally proposed by the European Commission on 24th September 2020 included a digital finance strategy, a proposal on markets in crypto assets (MiCA) and a proposal on distributed ledger technology.

What does DORA seek to achieve?

DORA seeks to raise awareness on ICT risk and works around the concept that ICT incidents and lack of operational resilience could possibly jeopardise the soundness of financial entities.

Which entities fall in scope?

Article 2 provides that the Regulation applies to credit institutions, payment institutions, account information service providers, e-money institutions, investment firms, crypto asset service providers, central securities depositories, central counterparties, trading venues, trade repositories, AIFMs, UCITS Management Companies, data reporting service providers, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries; institutions for occupational retirement pensions, credit rating agencies, administrators of critical benchmarks, crowdfunding service providers, securitization repositories and ICT third party service providers.

The following entities fall outside the scope of DORA:

(a) Managers of alternative investment funds referred to in Article 3(2) of Directive 2011/61/EU – small scope AIFMs.

(b) Insurance and reinsurance undertakings referred to in Article 4 of Directive 2009/138/EC[1];

(c) Institutions for occupational retirement provision which operate pension scheme which together do not have more than 15 members in total.

(d) Natural or legal persons exempted from the application of Directive 2014/65/EU pursuant to Articles 2 and 3 of that Directive[2];

(e) Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises, small or medium-sized enterprises.

(f) Institutions referred to in point (3) of Article 2(5) of Directive 2013/36/EU[3].

DORA seeks to classify financial entities into the following categories:

Microenterprise

- a financial entity which is not a trading venue, central counterparty, trade repository or a central securities depository,
- employes fewer than 10 persons and has an annual turnover and/or annual balance sheet total which does not exceed EUR 2 million

Small enterprise

- employing 10 or more persons but less than 50 person;
- annual turnover and/or balance sheet total in exceess of EUR 2 million but not exceeding EUR 10 million

Medium- sized enterprise

- not a small enterprise but employs less than 250 persons;
- annual turnover not exceeding EUR 50 million and/or an annual balance sheet which does not exceed EUR 43 million

Between June and December 2024, financial entities were expected by some home regulators to self-classify as microenterprise, small enterprise or medium-sized enterprise using the EU SME test.

[1] Article 4 lists the entities which are deemed to fall outside the scope of Solvency II due to size

[2] Articles 2 and 3 deal with the entities which are exempted from the scope of MiFID II

[3] Post office giro institutions

Which requirements does DORA impose on financial entities falling in scope?

In essence, financial entities will be expected to implement (subject to the application of the principle of proportionality) the following requirements:

ICT Risk Management [Articles 5 – 15]

Financial entities are expected to have in place internal governance and control frameworks to ensure an effective and prudent management of all ICT risks[4]. The management body of the financial entity is expected to define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework.

By now all financial entities including those classified as microenterprises should have a documented ICT risk management framework which should be reviewed at least annually or upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes.

The ICT risk management framework will also be subject to internal audit on a regular basis.

The ICT risk management framework also requires financial entities to identify, classify and adequately document the ICT supported business functions, roles and responsibilities, the information assets and ICT Assets supporting these functions, and their roles and dependencies with ICT risk. The adequacy of this classification shall be reviewed as necessary but at least on an annual basis [Article 8].

Financial entities are also expected to implement mechanisms to promptly detect anomalous activities including ICT network performance issues and ICT-Related incidents and to identify potential material single points failure. These detection mechanisms shall be regularly tested [Article 10].

Management, classification, and reporting of ICT-related incidents [Article 17 – Article 21]

Financial entities are expected to establish and implement an ICT-related incident management processes to detect, manage and notify ICT-related incidents and shall also implement early warning indicators as alerts. This can be attained if financial entities establish processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT related incidents, to make sure that root causes are identified and eradicated to prevent the occurrence of such incidents.

In addition, financial entities are required to classify ICT-related incidents and determine their impact based on pre-established criteria such as number and/or relevance of clients or of users or financial counterparts impacted, duration of downtime, geographical spread relating to the areas impacted by the ICT incident, data losses, criticality of services affected and the economic impact. [Article 18].

Simplified ICT Risk Management framework

Whilst articles 5 to 15 shall not apply to small and non-interconnected investment firms, payment institutions, institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the operation, electronic money institutions and small institutions for occupational retirement provision, nonetheless, financial entities are required to implement a sound and documented ICT risk management framework that details the mechanisms and measures aimed at a quick, efficient and comprehensive management of all ICT risks, including for the protection of relevant physical components and infrastructures. Furthermore such financial entities are expected to continuously monitor the security and functioning of all ICT systems. [Article 16].

[4] An ICT risk means any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialized, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes or of the provision of services by producing adverse effects in the digital or physical environment.

DORA further details the procedure to be followed in relation to the reporting of major ICT related incidents and voluntary notification of significant cyber threat to the relevant competent authority within prescribed timeframes. In the case of major ICT-related incidents, financial entities will be required to submit to the competent authority:

A) An initial notification.

B) An intermediate report, as soon as the status of the original incident has changed significantly, of the handling of the major ICT-related incident as changed based on new information available, after the initial notification referred to in point (a), followed as appropriate by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority.

C) A final report, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented and when the actual impact figures are available to replace estimates.

The information provided to the competent authority shall be such as to enable it to determine the significance of the major ICT-related incident and assess possible cross-border impacts.

Apart from reporting major ICT-related incidents, financial entities may, on a voluntary basis, notify the competent authority of relevant cyber threats when they deem the threat to be of relevant to the financial system, service users or clients.

The reporting process will also be subject to supervisory feedback by the competent authority which shall acknowledge receipt of the notification and shall provide feedback as quickly as possible to make available any relevant anonymized information and intelligence on similar threats, discuss remedies applied at the level of the entity and ways to minimize and mitigate adverse impact across financial sectors [Article 20].

Digital Operational Resilience Testing [Article 24 – Article 27]

Financial entities are required to have a sound and comprehensive digital operational resilience testing programme as part of the ICT risk management framework for the purposes of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies or gaps in the digital operational resilience and promptly implementing corrective measures [Article 24].

This shall include a range of assessments, tests, methodologies, practices, and tools to be applied in accordance with the methodology outlined in DORA. Financial entities shall follow a risk-based approach when conducting the digital operational resilience testing programme and shall ensure that tests are undertaken by independent parties whether internal or external.

All critical ICT systems and applications shall be tested at least on a yearly basis using the methodology outlined in Articles 25 and 25 of the Regulation.

Article 27 of the Regulation outlines the requirements for testers for the deployment of threat led penetration testing requiring these to be inter alia of the highest suitability and reputability and to be certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks.

Sound management of ICT third party risk [Article 28 – 30]

Financial entities are required to manage ICT third party risk as an integral component of ICT risk within their ICT risk management framework and shall always remain fully responsible for complying with and the discharge of all obligations under the Regulation and financial services legislation. The obligation of the management of ICT third party risk shall be implemented considering the principle of proportionality.

As part of the ICT risk management framework, financial entities are expected to adopt and regularly review a strategy on ICT third party risk. In addition, DORA introduces a reporting obligations through the Register of Information which financial entities are required to maintain and update at entity level and at sub-consolidated and consolidated levels including all contractual arrangements on the use of ICT services provided by ICT third-party service providers. Financial entities are expected to document appropriately these contractual arrangements distinguishing between critical and non-critical functions.

Furthermore, financial entities are required to:

(a) Report at least on an annual basis to the competent authorities information on the number of new arrangements on the use of ICT services, the categories of ICT third party service providers, the type of contractual arrangements and the services and functions which are being provided.

(b) Make available to the competent authority upon request, the full register of information as requested, specified sections thereof, along with any information deemed necessary to enable the effective supervision of the financial entity.

(c) Inform the competent authority in a timely manner about planned contracting of critical or important functions and when a function has become critical or important.

Article 30 provides for the key contractual provisions to be included as a minimum in the contract between the financial entity and the ICT Third-Party Service Provider whether these are critical or non-critical functions. In the case of critical or important functions, Article 27 further supplements the minimum requirements.

Which other areas does DORA tackle?

Section II of Chapter V deals with oversight framework of critical ICT third party service providers. The ESAs shall designate the ICT third party service providers which are critical for financial entities following an assessment which considers:

(a) The systemic impact on the stability, continuity, or quality of the provision of financial services in the case the relevant ICT third-party provider would face a large-scale operational failure to provide its services considering the number of financial entities and the total value of assets of financial entities to which the relevant ICT third party service provider provides services.

(b) The systemic character or importance of the financial entities that rely on the relevant ICT third party provider, assessed in accordance with the parameters of number of G-SIIs[5] and other O-SIIs[6] serviced and the interdependence between the G-SIIs or O-SIIs and other financial entities.

(c) The reliance of financial entities on the services provided by the relevant third-party service provider.

(d) The degree of substitutability.

The ESAs shall establish, publish, and update on an annual basis the list of critical ICTS third party service providers at EU level.

In relation to ICT third country service providers, the Regulation provides that financial entities shall only make use of the services of such a provider which has been designated as critical, if the latter has established a subsidiary in the Union within 12 months following the designation [Article 31(12)] so that oversight can be implemented properly.

[5] Global systemically important institutions.

[6] Other systemically important institutions

How does the principle of proportionality apply?

Given that the list of financial entities falling within the scope of DORA, the Regulation takes into consideration the principle of proportionality in Article 4. Furthermore, throughout the provisions, specific reference is made to the applicability of this principle as well as the need to distinguish between microenterprises[7] and small[8] and medium-sized enterprises[9]. The below seeks to illustrate the applicability of the principle of proportionality throughout the Regulation.

The applicability of the principle of proportionality throughout the Regulation

Chapter I - General Provisions	• Applicable across the board
Chapter II - ICT Risk management	• Implementation shall be in accordance with the principle of proportionality, taking into account size, nature, scale and complexity of services, activities and operations and the overall risk profile.
Chapter III - ICT related incidents management, classification and reporting	• Implementation shall be proportionate to the size and overall risk profile, and to the nature, scale and complexity of the services, activities and operations of the financial entity as provided in the articles of this chapter.
Chapter IV - Digital operational resilience testing	• Implementation shall be proportionate to the size and overall risk profile, and to the nature, scale and complexity of the services, activities and operations of the financial entity as provided in the articles of this chapter.
Chapter V - Section 1 - Key Principles for a sound management of ICT third party risk	• Implementation shall be proportionate to the size and overall risk profile, and to the nature, scale and complexity of the services, activities and operations of the financial entity as provided in the articles of this chapter.

[7] A microenterprise means a financial entity other than a trading venue, a central counterparty, a trade repository, or a central securities depository which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

[8] A small enterprise is a financial entity that employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.

[9] Medium-sized enterprise means a financial entity that is not a small enterprise and employs fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million and/or an annual balance sheet total not exceeding EUR 43 million.

Which additional technical standards are supplementing DORA?

DORA should also be read in conjunction with the following:

- Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework;
- Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents;
- Commission Delegated Regulation (EU) 2025/301 of 23 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats;
- Commission Implementing Regulation (EU) 2025/302 of 23 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat;
- Commission Delegated Regulation (EU) .../... supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria used for identifying financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to the scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition; **– This is not yet in force**
- Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers;
- Commission Delegated Regulation (EU) .../... supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the elements that a financial entity has to determine and assess when subcontracting ICT services supporting critical or important functions; **– This is not yet in force**
- Commission Implementing Regulation (EU) 2024/2956 of 29 November 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to standard templates for the register of information;
- Commission Delegated Regulation (EU) 2025/295 of 24 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards on harmonisation of conditions enabling the conduct of the oversight activities;
- Commission Delegated Regulation (EU) 2025/420 of 16 December 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards to specify the criteria for determining the composition of the joint examination team ensuring a balanced participation of staff members from the ESAs and from the relevant competent authorities, their designation, tasks and working arrangements.

Which regulatory authorities will be the designated competent authorities?

Article 46 of the Regulation provides considerable detail in relation to the designated competent authorities. In relation to investment firms and management companies, compliance with the provisions of the Regulations shall be ensured but the following competent authorities:

Financial entity	Designated Competent Authority
Investment Firms	The competent authority designated in accordance with Article 4 of Directive (EU) 2019/2034.
AIFMs	The competent authority designated in accordance with article 44 of Directive 2011/61/EU
UCITS Management Companies	The competent authority designated in accordance with Article 97 of Directive 2009/65/EC

What should financial entities do now?

The implementation deadline for DORA was 17th January 2025 and ahead of that date financial entities falling in scope should have been updating their internal policies and procedures amongst which the ICT policy, Outsourcing Policy and Register and Business Continuity Arrangements. Furthermore, the necessary governance arrangements should have also been implemented and approved by senior management and the governing bodies of these entities.

How can Apex help?

Apex Group can help by assisting in:

- Gap analysis
- Drafting and updating of policies
- Compiling and submitting the Register of Information

apexgroup.com

Contact us | Disclaimer

5429_160425