E-BOOK

APEX

Digital Operations Resilience Act

Introduction

The Digital Operational Resilience Act ("DORA") is designed to ensure that the European financial sector can maintain resilient operations in the case of a severe operational disruption. On 10th May 2022, the European Council and the European Parliament reached a provisional agreement on this legislative text which aims at outlining uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provider ICT related services such as cloud platforms or data analytics services. 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?

The proposal seeks to address in an adequate and comprehensive manner digital risks to all financial entities stemming from an increased use of information and communication technology in the provision and consumption of financial services, thereby contributing to the culmination of the potential digital finance in terms of innovation and competition.

Which entities fall in scope?

Article 2 provides that the Regulation applies to credit institutions, payment institutions, 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]

Member States are given the discretion to exempt the following institutions that are located within their respective territory from the scope of the Regulation and in such case, they will be deemed to fall out of scope.

[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 4 – 14]

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 or the board of directors in the case of smaller set-ups will be responsible to define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework.

Save for financial entities which qualify as microenterprises,[5] the proposal is very prescriptive on the obligations of the management body in relation to the implementation of the ICT risk management framework and such entities are similarly required to establish a role to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services or to designate a member from senior management as responsible for overseeing the related risk exposure and relevant documentation.

The ICT risk management framework shall be documented and reviewed at least on an annual basis or periodically, in the case of microenterprises, as well as 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.

A report on the review of the ICT risk management framework shall be submitted to the competent authority upon request.

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 7].

Mechanisms shall also be implemented 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.

Simplified ICT Risk Management framework

Whilst articles 4 to 14 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 [Article 14a].

Management, classification, and reporting of ICT-related incidents [Article 15 – Article 20]

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 of users or financial counterparts impacted, duration of downtime, geographical spread relating to the areas impacted by the ICT incident [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.

[5] A microenterprise is 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.

The text of the Regulation 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 21 – Article 24]

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 21].

This shall include a range of assessments, tests, methodologies, practices, and tools to be applied in accordance with the methodology outlined in the Regulation. 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 22 and 23 of the Regulation.

Article 24 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 25 – 27]

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 will also adopt and regularly review a strategy on ICT third party risk. In addition, such entities will maintain and update a Register of Information in relation to all contractual arrangement on the use of ICT services provided by ICT third party service providers. These contractual arrangements shall be appropriately documented 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 27 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 2 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[6] and other O-SIIs[7] 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 28(9)] so that oversight can be implemented properly.

[6] Global systemically important institutions

[7] 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 3a of the text. Furthermore, throughout the provisions, specific reference is made to the applicability of this principle as well as the need to distinguish between microenterprises[8] and small[9] and medium-sized enterprises[10] e.g., Article 16. The below seeks to illustrate the applicability of the principle of proportionality throughout the Regulation.

Chapter 1 General Provisions	• Applicable across the board
Chapter 2 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 3 ICT related incidents management, classification, and reporting	• 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 as provided in the articles of this chapter.
Chapter 4 Digital operational resilience testing	• 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 as provided in the articles of this chapter.
Chapter 5 Section 1 Key Principles for a sound management of ICT third party risk	• 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 as provided in the articles of this chapter.

Which additional RTSs should financial entities expect?

Financial entities should also monitor the following RTSs and Delegated Acts which will be published during the next two years and which will further supplement the provisions of the Regulation:

Title	Article	RTS	Est. Date of Publication
ICT Risk management framework	Article 5(6)	RTSs to specify further the content and format of the report on the review of the ICT risk management framework	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation
Protection and Prevention	Article 8(2)	RTS on the elements to be included in the ICT security policies, procedures, protocols, and tools referred to in Article 8(2)	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation
	Article 8(4)	RTSs on the controls of access management rights as per Article 8(4)(c).	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation
Detection	Article 9(1)	RTS developing further the elements to enable a prompt detection of anomalous activity	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation
	Article 9(2)	RTSs developing the elements triggering ICT related incident detection and response processes	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation

[8] 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.

[9] 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.

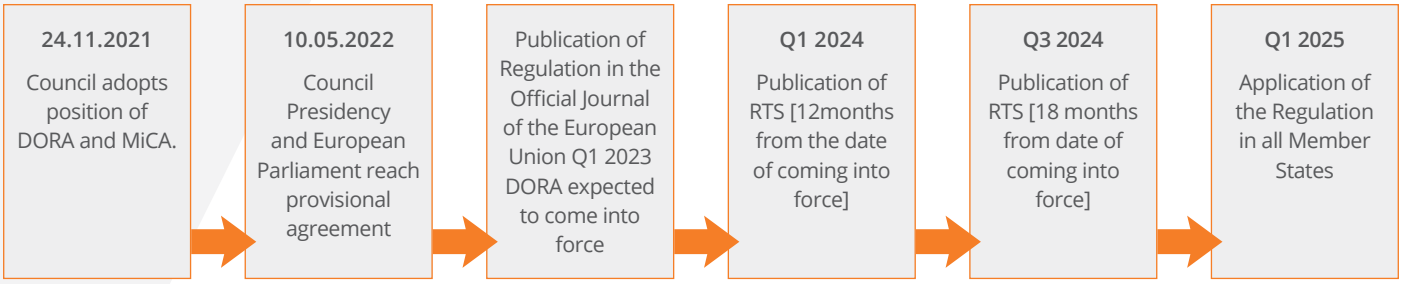
[10] Medium-sized enterprise means a financial entity that is not a small enterprise and employs fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million and/or an annual balance sheet total not exceeding EUR 43 million.

Title	Article	RTS	Est. Date of Publication
Response and recovery	Article 10(1)	RTS to specify further the components of the ICT business continuity policy	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation
	Article 10(5)	RTSs specifying further the testing of ICT business continuity plans	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation
Detection	Article 10(3)	RTSs to specify further the components of the ICT response and recovery plans	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation
	Article 10(9a)	The ESAs shall through the Joint Committee develop common guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents as reportable to competent authorities upon request.	To be submitted to the European Commission by 18 months after date of entry into force of the Regulation.
Simplified ICT Risk management framework	Article 14a(3)	RTSs to specify the elements to be included in the ICT risk management framework, the elements in relation to systems, protocols, and tools to minimize the impact of ICT risks, to specify further the components of the ICT business continuity plans and the rules on the testing of the business continuity plans and to specify the content and format of the report on the review of the ICT risk management framework.	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation
Classification of ICT related incidents and cyber threats	Article 16(2)	Draft RTSs on the criteria of Article 16(1) including materiality thresholds for determining major ICT related incidents and the criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT related incidents, and the criteria based on which cyber threats are classified as significant including high materiality thresholds.	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation
Harmonization of reporting content and templates	Article 18	ESAs shall develop RTSs to: • Establish the content of the reporting for major ICT-related incidents • Determine the time-limits for the initial notification and each report • Establish the content of the notification for significant cyber-threats • Establish the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and notify a significant cyber threat	To be submitted to the European Commission by 18 months after date of entry into force of the Regulation

Title	Article	RTS	Est. Date of Publication
Advanced testing of ICT tools, systems and processes based on threat led penetration testing	Article 23	RTS to further specify • The criterial used for the purpose of the application of Article 23(3b) relating to the power of the competent authority to delegate the exercise of threat led penetration testing to other national authorities in the financial sector • The requirements and standards governing the use of internal testers • The requirements relating to the scope of threat led penetration testing, the testing methodology and approach to be followed for each specific phase of the testing process and the results, closure, and remediation stages of the testing • The type of supervisory and other relevant cooperation needed for the implementation of threat led penetration testing and for the facilitation of mutual recognition of that testing, in the context of financial entities that operate in more than one Member State, to allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub- sectors or local financial markets.	To be submitted to the European Commission by 18 months after date of entry into force of the Regulation
General Principles – Sound management of ICT third party risk	Article 25	Development of RTSs to establish • The standard templates for the purposes of the register of information including information that is common to all contractual arrangement on the use of ICT Services • The content of the policy in relation to the contractual arrangements on the use of ICT services concerning critical or important functions provided by ICT third-party service providers.	To be submitted to the European Commission by 12 months after date of entry into force of the Regulation
Key contractual provisions	Article 27	RTSs to specify further the elements which a financial entity needs to determine and assess when subcontracting critical or important functions.	To be submitted to the European Commission by 18 months after date of entry into force of the Regulation
Designation of critical ICT third-party service providers	Article 28	Delegated act to supplement the Regulation specifying further the criteria to be taken into consideration when designating an ICT service provider as critical.	To be adopted within 18 months from the date of entry into force of the Regulation

When will DORA come into force?

DORA will apply within 24 months from the date of publication in the official journal. The below shows a timeline of events.



Which regulatory authorities will be the designated competent authorities?

Article 41 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

Which other pieces of legislation will DORA impact?

The Regulation will be supplemented by a Directive amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341. This Directive puts forward a set of amendments aimed at bringing legal clarity and consistency in relation to the application by financial entities that are authorised and supervised in accordance with the aforementioned Directives on the various requirements relating to digital operational resilience which are necessary in the provision of their activity.

What should financial entities do now?

Those financial entities falling in scope of DORA should not wait for the coming into force of this Regulation but should start assessing the implications of the new requirements now to identify any potential compliance gaps. Financial entities should consider their current governance arrangements and start discussing possible changes to ensure compliance with the provisions of the Regulation. Overall boards should start discussing and planning a clear compliance strategy which will be implemented during the 24-month implementation period window taking into consideration the RTSs which will be published by the ESAs as well as the publications and the circulars issued by the local regulators.

Contact

Isabelle Agius – Head of Regulatory Services, Apex Compliance Services
Malta Contact: isabellaagius@apexfunds.com.mt

apexgroup.com

Contact us | Disclaimer