DORA: THE EU'S NEW REGULATORY FRAMEWORK ON DIGITAL OPERATIONAL RESILIENCE

Following its publication in the Official Journal of the European Union on 27 December 2022, the Digital Operational Resilience Act (DORA)[1] and the DORA Amending Directive[2] entered into force on 16 January 2023 and will apply from 17 January 2025.

DORA sets 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 provide Information Communication Technology (ICT)-related services to them, such as cloud platforms or data analytics services.

DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats. These requirements are homogenous across all EU member states. The core aim is to prevent and mitigate cyber threats.

Background to DORA

The European Commission (the Commission) came forward with the DORA proposal[3] on 24 September 2020 as part of a larger digital finance package, which aims to develop a European approach that fosters technological development and ensures financial stability and consumer protection.

In addition to DORA, the digital finance strategy contains a proposal on markets in crypto-assets[4] (MiCA) and a proposal on distributed ledger technology[5] (DLT Pilot Regime).

The package aims to support innovation and the uptake of new financial technologies while providing for an appropriate level of consumer and investor protection by bridging gaps in existing EU legislation, thereby ensuring that the current legal framework does not pose obstacles to the use of new digital financial instruments and, at the same time, ensures that new technologies and products fall within the scope of financial regulation and operational risk management arrangements of firms active in the EU.

Purpose and scope

DORA covers a very wide range of financial entities regulated in the EU, for example investment firms, managers of alternative investment funds, management companies, credit institutions, central securities depositories, amongst many others. It also applies to ICT third-party services providers, including those established in third countries that provide services to captured entities within the EU. A full list of the entities subject to the DORA Regulation can be found in DORA Article 2 (Scope).

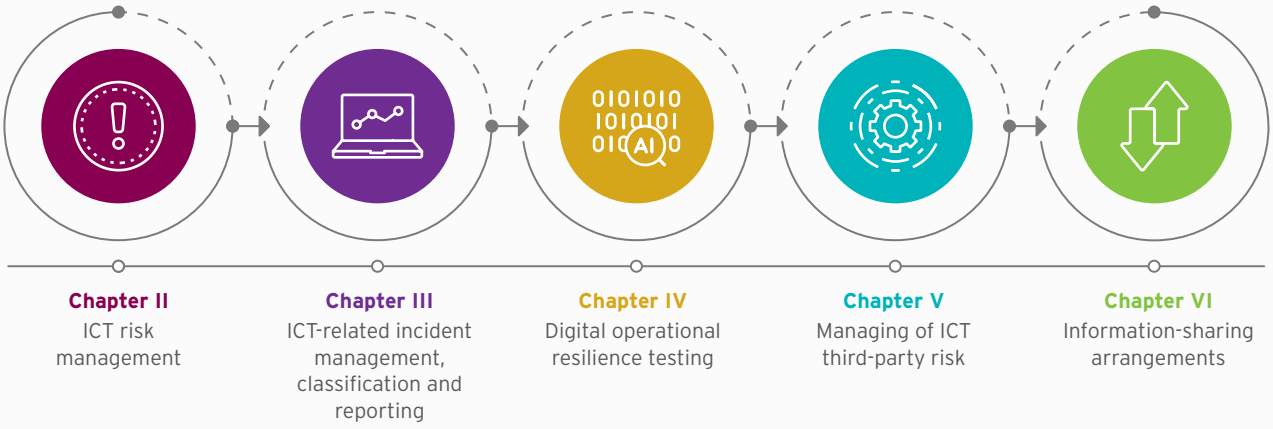
The Commission recognises that significant differences exist between financial entities in terms of size, business profiles, or in relation to their exposure to digital risk. As a result, DORA takes steps to drive a proportionate, risk-based approach to ICT risk oversight.

DORA is designed to better align financial entities' business strategies and the conduct of ICT risk management.

DORA will create a comprehensive framework addressing various, core components of the digital operational resilience of financial entities. It will enhance the overall conduct of ICT risk management, establish testing rules for ICT systems, increase financial supervisors' awareness of cyber risks through an EU harmonised incident reporting scheme and introduce EU oversight to oversee financial entities' dependency on ICT third-party service providers.

The overall objective is to strengthen and align digital operational resilience across EU financial services sector.

Key requirements in DORA



Chapter II
ICT risk management

Chapter III
ICT-related incident management, classification and reporting

Chapter IV
Digital operational resilience testing

Chapter V
Managing of ICT third-party risk

Chapter VI
Information-sharing arrangements

ICT risk management

Section I of Chapter II covers governance and organisation where financial entities will need to have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in order to achieve a high level of digital operational resilience.

The management body of the financial entity will also need to define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework. The management body shall bear the ultimate responsibility for managing the financial entity's ICT risk and for putting in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data.

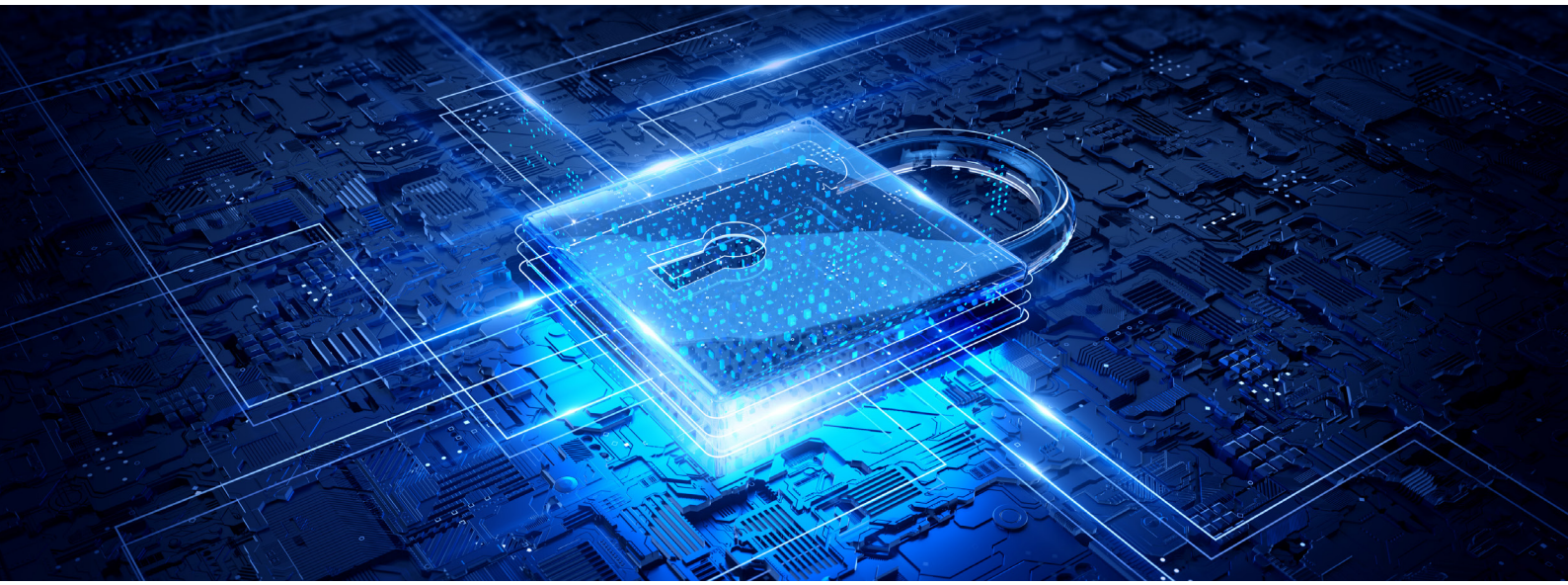
Additionally, Section II of Chapter II covers the ICT risk management framework; ICT systems, protocols and tools; identification; protection and prevention; detection; response and recovery; backup policies and procedures; restoration and recovery procedures and methods; learning and evolving; communication; further harmonisation of ICT risk management tools, methods, processes and policies; and a simplified ICT risk management framework.

Further details on these requirements can be found in DORA Articles 5-16.

ICT-related incident management, classification and reporting

Financial entities are required to define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents, as well as record all ICT-related incidents and significant cyber threats. They will also need to classify ICT-related incidents and determine their impact based on criteria set out in DORA.

Also set out in DORA are the requirements for the reporting of major ICT-related incidents and voluntary notification of significant cyber threats. The initial notification and reports will need to include all information necessary for the national competent authority (NCA) to determine the significance of the major ICT-related incident and assess possible cross-border impacts.



Financial entities may, on a voluntary basis, notify significant cyber threats to the relevant NCA when they deem the threat to be of relevance to the financial system, service users or clients.

Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident.

In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking.

Further details on these requirements can be found in DORA Articles 17-23.

Digital operational resilience testing

For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities, other than microenterprises, shall, taking into account the criteria set out in DORA Article 4(2), establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework.

The digital operational resilience testing programme referred to in DORA Article 24 shall provide for the execution of appropriate tests, such as vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.

Further details on these requirements can be found in DORA Articles 24-27.

Managing of ICT third-party risk

DORA splits out the requirements for managing ICT third-party risk into two sections. Section I addresses the key principles for a sound management of ICT third-party risk, and Section II the oversight framework of critical ICT third-party service providers.

The key principles state that financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall, at all times, remain fully responsible for compliance with, and the discharge of, all obligations under DORA and applicable financial services law.

Financial entities' management of ICT third-party risk shall be implemented proportionately, taking into account:

- The nature, scale, complexity and importance of ICT-related dependencies; and
- The risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, factoring in the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities, at individual and at group level.

As set out in DORA Article 30, the rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing.

Within Section II, the oversight framework of critical ICT third-party service providers covers the following areas:

- Designation of critical ICT third-party service providers, including limitations on the use of ICT service providers established in a third country;
- Structure of the Oversight Framework;
- Tasks of the Lead Overseer[6];
- Operational coordination between Lead Overseers;
- Powers of the Lead Overseer;
- Exercise of the powers of the Lead Overseer outside the EU;

- 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; and
- International cooperation.

Further details on these requirements can be found in DORA Articles 28-44.

Information-sharing arrangements

Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:

- Aims to enhance the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages;
- Takes place within trusted communities of financial entities; and
- Is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data in accordance with the General Data Protection Regulation[7] and guidelines on competition policy.

Further details on these requirements can be found in DORA Article 45.

DORA Amending Directive

In addition to the DORA Regulation, the Commission published at the same time the DORA Amending Directive that includes amendments to eight Directives, including the UCITS Directive, AIFMD, and MiFID II. The purpose of the DORA Amending Directive is to ensure legal clarity by introducing cross-references in the relevant Directives to DORA.[8]

The transposition and timing of the DORA Amending Directive aligns with that of the DORA Regulation, with the NCAs of EU Member States required to adopt and publish the measures necessary to comply with the DORA Amending Directive by its application date of 17 January 2025.

DORA and ESMA's AWP

Prior to the formal adoption of DORA, on 10 October 2022, ESMA published its 2023 Annual Work Programme (AWP).[9] The AWP sets out ESMA's priority work areas for 2023 to deliver on its mission to enhance investor protection and promote stable and orderly financial markets.

DORA is represented in the AWP under the key deliverable of facilitating technological innovation and the effective use of data (alongside MiCA and the DLT Pilot Regime).

Many of ESMA's mandates under DORA will also be implemented in cooperation with its fellow regulators – the EBA and EIOPA and include:

- A feasibility study for the development of a centralised system for reporting of major ICT-related incidents;
- The preparation for the oversight function foreseen for the three ESAs[10]; and
- The development of several technical standards, guidelines and reports.

The mandates will be delivered in 2023 and in 2024 and cover topics such as ICT risk management, incident reporting, threat-led penetration testing, and third-party risk management.

ESAs to begin their work now

In a letter to the ESA's[11], published on 4 January 2023 (dated 21 December 2022), the Commission wrote with a request for advice[12] regarding designation criteria and fees for the DORA oversight framework.

DORA empowers the Commission to adopt two delegated acts to further specify the designation criteria for critical ICT third-party service providers (CTPPs) and the amount of fees to be levied on such providers. In this context, the Commission has requested the ESAs to provide advice on further specifying the details aimed at shaping-up the designation criteria for CTPPs, as well as the elements which are needed in the specification of the amount of the fees, and the way and methods in which such fees are to be paid.

For DORA to be fully operational and the ESAs to initiate their oversight activities, the Commission has requested the ESAs start working on their request as soon as possible. The deadline set to the ESAs to deliver the technical advice is 30 September 2023.

Next steps

Now that DORA is in force, aspects that require national transposition (such as changes to the UCITS Directive and AIFMD as a result of the DORA Amending Directive) will be passed into law by each EU member state by 17 January 2025. At the same time, the ESAs will develop technical standards for all financial services institutions to abide by, from banking to insurance to asset management.

Impacted financial entities will now need to conduct a gap analysis of the final rules against their current processes and procedures relating to their ICT risk management framework in order to identify any areas where work may be required to ensure compliance with DORA before its application date.

Any review should also include a reassessment, and where necessary renegotiation, of financial entities agreements with their third-party ICT service providers to ensure compliance with DORA before the 17 January 2025.

---

1. See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=EN.
2. See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2556&from=EN.
3. See Digital finance package (europa.eu).
4. Ibid.
5. Ibid.
6. 'Lead Overseer' means the European Supervisory Authority appointed in accordance with DORA Article 31(1), point (b).
7. See General data protection regulation (GDPR) (europa.eu).
8. For example, the UCITS Directive Article 12(1)(a) is amended to ensure the UCITS or UCITS management company has sound administrative and accounting procedures, control and safeguard arrangements for electronic data processing, including with regard to network and information systems that are set up and managed in accordance with DORA.
9. See AWP 2023 (europa.eu).
10. European Supervisory Authorities (ESAs): the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA).
11. See transmission letter CfA – DORA.pdf (europa.eu).
12. See Draft ESAs technical advice_commented by ESAs (europa.eu).

Please contact for further details:

David Morrison
Global Head of Trustee and Fiduciary Services
david.m.morrison@citi.com
+44 (0) 20 7500 8021

Ann-Marie Roddie
Head of Product Development Fiduciary Services
annmarie.roddie@citi.com
+44 (1534) 60-8201

Amanda Hale
Head of Regulatory Services
amanda.jayne.hale@citi.com
+44 (0)20 7508 0178

Caroline Chan
APAC Head of Fiduciary Business
caroline.mary.chan@citi.com
+852 2868 7973

Shane Baily
EMEA Head of Trustee and Fiduciary Services
UK, Ireland and Luxembourg
shane.baily@citi.com
+353 (1) 622 6297

Jan-Olov Nord
EMEA Head of Fiduciary Services
Netherlands and Sweden
janolov.nord@citi.com
+31 20 651 4313

cbs37125 02/23