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.

In this e-briefing, we look at the background to DORA, the regulation itself, and the current status of the level two and three proposals as we approach DORA's application in January 2025.

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 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 DORA can be found in DORA Article 2 (Scope).

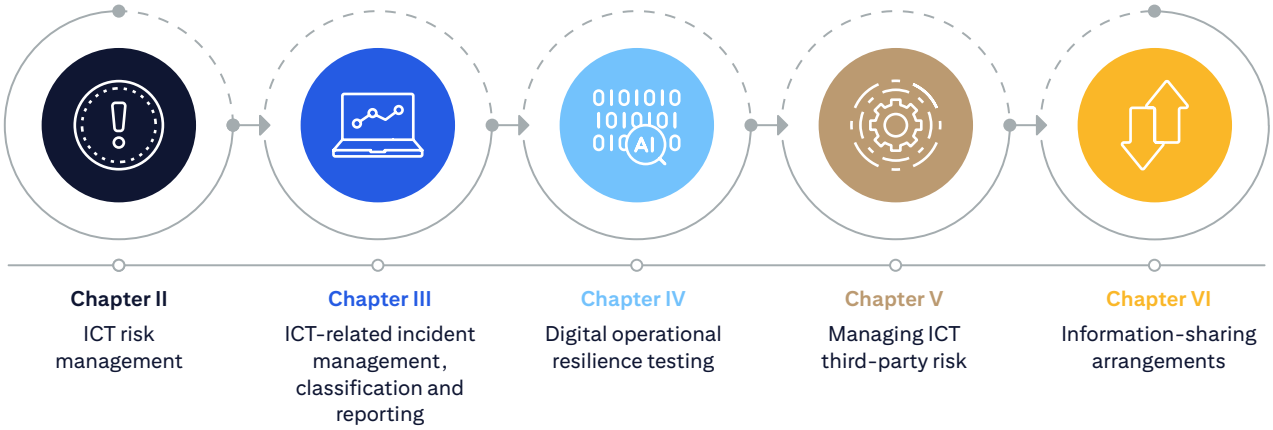
The Commission recognises that significant differences exist between financial entities in terms of size, business profiles, or in relation to their exposure to digital risk. As a result, DORA takes steps to drive a proportionate, risk-based approach to ICT risk oversight.

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 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 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.

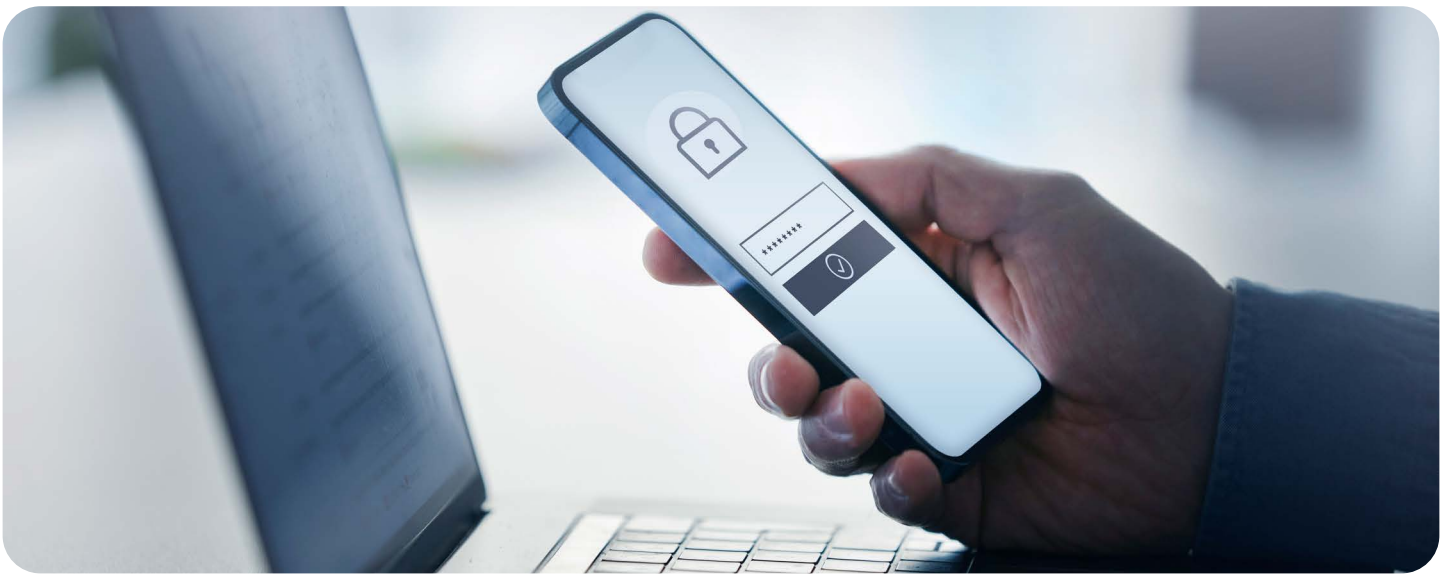
ICT-related incident management, classification, and reporting

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 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.

Joint technical advice

On 29 September 2023, the European Supervisory Authorities (ESAs) published technical advice[9], responding to the Commission's December 2022 Call for Advice on two delegated acts specifying further criteria for critical ICT third-party service providers and determining oversight fees levied on such providers, under Articles 31 and 43 of DORA.

Both delegated regulations were adopted on 22 February 2024 and published in the EU's Official Journal on 30 May 2024.[10]

The delegated regulation ((EU) 2024/1502),specifying the criteria for the designation of ICT third-party service providers as critical for financial entities, covers: assessment approach; systemic impact of ICT third-party service providers on the stability; continuity or quality of the provision of financial services; systemic character and importance of the ICT services provided to financial entities; criticality or importance of the functions; degree of substitutability; and information sources to enable criticality assessment.

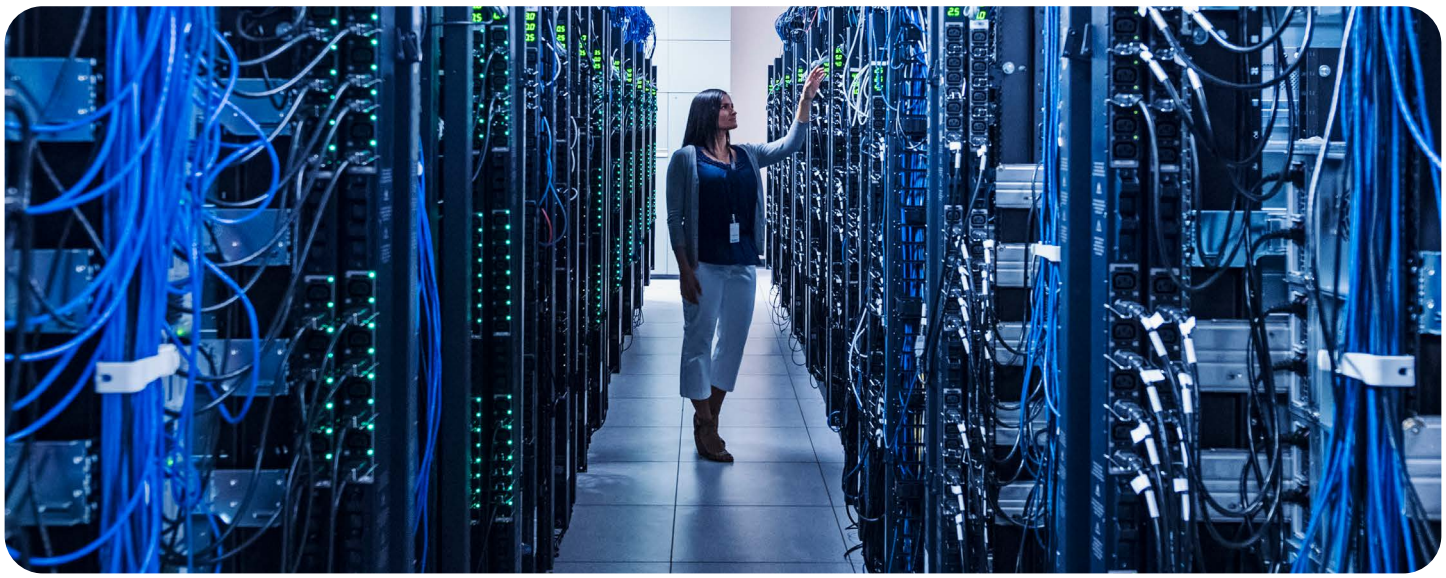
Whilst the delegated regulation ((EU) 2024/1505) determining the amount of the oversight fees to be charged by the Lead Overseer[11] (LO) to critical ICT third-party service providers and the way in which those fees are to be paid, covers: estimation of the expenditures of the LO when performing their oversight duties; applicable turnover of critical ICT third-party service providers for the calculation of the oversight fees; calculation of the oversight fees; oversight fees in year of designation and 'opt-in' requests; payment of the oversight fees; and communication between the LO and critical ICT third-party service providers.

First batch of technical standards

On the 17 January 2024, the ESAs published the first set of final draft technical standards[12] under DORA.

The joint final draft technical standards include:

- Regulatory Technical Standards (RTS) on ICT risk management framework and on simplified ICT risk management framework;
- RTS on criteria for the classification of ICT-related incidents;
- RTS to specify the policy on ICT services supporting critical or important functions provided by ICT third-party service providers (TPPs); and
- Implementing Technical Standards (ITS) to establish the templates for the register of information.



RTS on ICT risk management framework and on simplified ICT risk management framework ((EU) 2024/1774)

This RTS covers:

- Harmonisation of ICT risk management tools, methods, processes, and policies covering:
  - ICT Security policies, procedures; protocols, and tools, including:
    - General elements of ICT security policies, procedures, protocols, and tools;
    - ICT risk management;
    - ICT asset management;
    - Encryption and cryptography;
    - ICT operations security;
    - Network security;
    - ICT project and change management; and
    - Physical and environmental security.
  - Human resources policy and access control;
  - ICT-related incident detection and response;
  - ICT business continuity management; and
  - Report on the ICT risk management framework review.
- Simplified ICT risk management framework for financial entities captured under Article 16(1) of DORA[13], covering:
  - Simplified ICT risk management framework;
  - Further elements of systems, protocols, and tools to minimise the impact of ICT risk;
  - ICT business continuity management; and
  - Report on the review of the simplified ICT risk management framework.

RTS on criteria for the classification of ICT-related incidents ((EU) 2024/1772)

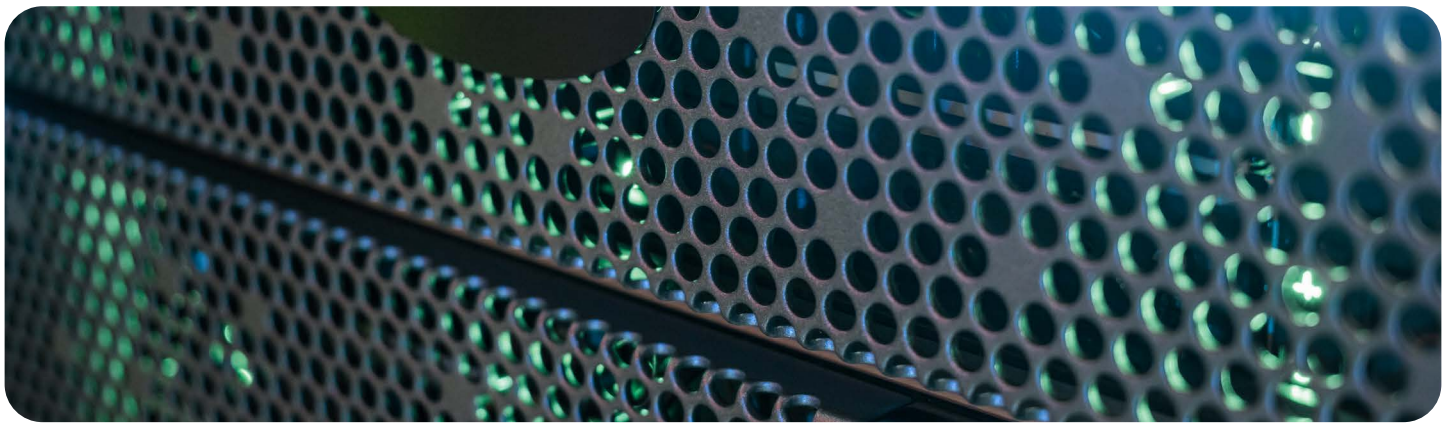
In the press release accompanying the draft rules, published on 17 January 2024, ESMA stated that the "RTS ensure a harmonised and simple process of classifying incident reports throughout the financial sector."[14]

The RTS 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, covers:

- Classification criteria, covering:
  - Clients, financial counterparts and transactions;
  - Reputational impact;
  - Duration and service downtime;
  - Geographical spread;
  - Data losses;
  - Criticality of services affected; and
  - Economic impact.
- Major incidents and materiality thresholds for determining major incidents;
- High materiality thresholds for determining significant cyber threats;
- Relevance of major incidents to competent authorities in other Member States; and
- Details of major incidents to be shared with other competent authorities.

RTS to specify the policy on ICT services supporting critical or important functions provided by ICT TPPs ((EU) 2024/1773)

ESMA states that the RTS "aim to ensure financial entities remain in control of their operational risks, information security and business continuity throughout the life cycle of contractual arrangements with such ICT third-party service providers."[15]



The RTS covers:

- Overall risk profile and complexity;
- Group application;
- Governance arrangements;
- Main phases of the life cycle for the adoption and use of contractual arrangements;
- Ex-ante risk assessment;
- Due diligence;
- Conflicts of interest;
- Contractual clauses;
- Monitoring of the contractual arrangements; and
- Exit from and termination of the contractual arrangements.

ITS on the register of information

The draft ITS sets out the templates to be maintained and updated by financial entities in relation to their contractual arrangements with ICT third-party service providers.

The ESAs state that the "register of information will play a crucial role in the ICT third-party risk management framework of the financial entities and will be used by competent authorities and ESAs in the context of supervising financial entities' compliance with DORA and to designate critical ICT third-party service providers that will be subject to the DORA oversight regime."

Next steps

The three RTS were adopted on 13 March 2024 and published in the EU's Official Journal on 25 June 2024.[16] They came into force on 15 July 2024.

However, the ITS to establish the templates for the register of information, at the time of writing this e-briefing, had still to be adopted.

Second batch of technical standards

On 17 July 2024, the ESAs published the second batch of policy documents under DORA.

This batch consists of four final draft RTS, one final draft ITS and two Joint Guidelines.

RTS and ITS on the content, format, templates, and timelines for reporting major ICT-related incidents and significant cyber threats[17]

The RTS cover the content of reports for major ICT-related incidents to reflect criteria laid down in Article 18(1) of DORA[18] and incorporate further elements such as details for establishing the relevance of the reporting for other Member States and whether it constitutes a major operational or security payment-related incident or not. They also determine time limits for the initial notification and for each report referred to in Article 19(4)[19], as well as establishing the content of the notification for significant cyber threats.

The ITS provide standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat.

RTS on the harmonisation of conditions enabling the conduct of the oversight activities[20]

The RTS includes:

- Information to be provided by ICT third-party service providers in the application for a voluntary request to be designated as 'critical'.
- Information that critical third-party service providers must provide to the LO. That is the specific ESA designated as such.
- Criteria for determining the composition of the joint examination, ensuring a balanced participation of staff members from the ESA and from the relevant competent authorities, their designation, tasks and working arrangements.
- Details of the NCA's assessment of measures taken by critical third-party providers based on the recommendations of the LO.

RTS specifying the criteria for determining the composition of the joint examination team (JET)[21] – Article 41(1)(c) of DORA

- The information to be provided by an ICT third-party service provider in the application for a voluntary request to be designated as critical;
- The information to be submitted by the ICT third-party service providers that is necessary for the LO to carry out its duties;
- The criteria for determining the composition of the joint examination team, their designation, tasks, and working arrangements; and
- The details of the competent authorities' assessment of the measures taken by critical third-party providers (CTPPs) based on the recommendations of the LO.

RTS on elements related to threat-led penetration testing (TLPT)[22]

The ESAs were authorised to deliver RTS on certain aspects of advanced testing of ICT tools, systems and processes based on Threat-led Penetration Testing (TLPT). These RTS were required to be in accordance with the TIBER-EU framework.[23]

The RTS provide information relating to definitions of key terms, the identification of financial entities who are required to perform TLPT, details around testing methodology – including organisational arrangements for financial entities, risk management for TLPT – including for pooled and joint TLPTs.

A section on the testing process, including 1) the preparation phase, 2) the testing in terms of threat intelligence providers, 3) red team tests, 4) closure phase and 5) remediation plan.

Finally, requirements and standards governing the use of internal testers, and cooperation with TLPT authorities in different member states.

Given the highly technical nature of the RTS, there are also annexes covering the contents of: the project charter; scope application document; targeted threat intelligence reports; red team test plans and reports; blue team test reports[24]; details of the report summarising the relevant findings of the TLPT; and details of the attestation of the TLPT.

ITS on reporting details for major ICT-related incidents[25]

The ITS cover the content of the required notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents.

The ITS also include standard forms, templates, and procedures for financial entities to report a major incident and to notify a significant cyber threat.

Finally, the Joint Guidelines include:

Guidelines on the estimation of aggregated costs/ losses caused by major ICT-related incidents[26]

Financial entities should estimate the aggregate annual costs and losses of major ICT-related incidents by aggregating the costs and losses for major ICT-related incidents that fall within the reference year for which the competent authority requested the estimation.

In addition, the Guidelines provide further details on sequential steps that firms should take to estimate the aggregated costs and losses. The Guidelines Annex further provides a reporting template that should be used.

Guidelines on oversight cooperation[27]

These Guidelines deal with the cooperation between the ESAs and the NCAs, covering the detailed procedures and conditions for the allocation and execution of tasks between NCAs and the ESAs and the details on the exchanges of information which are necessary for NCAs to ensure the follow-up of recommendations addressed to CTPPs.

RTS on sub-contracting

On 26 July 2024, the ESAs published a joint final Report on the draft RTS on sub-contracting under DORA.[28]

The RTS focus on ICT services provided by ICT sub-contractors that support 'critical' or 'important' functions, or material parts of them, and specify how to determine and assess the conditions for sub-contracting ICT services that support 'critical' or 'important' functions under DORA.

In addition, the RTS specify the requirements throughout the lifecycle of contractual arrangements between financial entities and ICT third-party service providers.

They require financial entities to take account of:

- The overall risk profile and complexity of the financial entity and the nature, scale, and elements of increased or reduced complexity of its services, activities, and operations;
- A group application requirement;
- Due diligence and risk assessment regarding the use of sub-contractors supporting critical or important functions;
- The description and conditions under which ICT services supporting a critical or important function can be sub-contracted;
- Conditions for sub-contracting relating to the chain of ICT sub-contractors providing a service supporting a critical or important function by the financial entity;
- Material changes to sub-contracting arrangements of ICT service supporting critical or important functions; and
- Termination of the contractual arrangement.

Next steps

The draft RTS and ITS have been submitted to the Commission to review, with the objective to adopt them to be effective from 17 January 2025, in line with the effective date of DORA.

Local regulatory engagement

In terms of local regulatory commentary on firms' preparations for the DORA deadline, on 1 July the Central Bank of Ireland published a speech on implementing DORA[29], delivered by Gerry Cross at the "6-Months to DORA" event.[30]

Then on 5 July 2024, the Dutch Authority for the Financial Markets (AFM) published guidance following its review of how financial service providers, capital market participants, and investment firms scored themselves in relation to DORA implementation. The output of this has resulted in ten key DORA-related themes.[31]

Whilst the AFM's coverage is not exhaustive, firm's may find the AFM output and associated checklist useful in assessing their own preparations for DORA.

Finally, on 19 August 2024, the Luxembourg Regulator, the Commission de Surveillance du Secteur Financier (CSSF), launched a DORA Readiness Survey, to raise awareness and assess readiness prior to DORA's application.[32]

[1] See Publications Office (europa.eu)

[2] See Publications Office (europa.eu)

[3] See Digital finance package - European Commission (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 Joint-ESAs__response_to_the_Call_for_advice_on_the_designation_criteria_and_fees_for_the_DORA_oversight_framework_final.pdf (europa.eu)

[10] See Access the Official Journal – EUR-Lex (europa.eu), 30 May 2024

[11] The LO is the relevant ESA appointed in accordance with Article 31(1), point (b) of DORA and will conduct the oversight of the assigned critical ICT third-party service providers and shall be, for the purposes of all matters related to the oversight, the primary point of contact for those critical ICT third-party service providers.

[12] See Esma Library | European Securities and Markets Authority (europa.eu)

[13] Defined as "small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366; institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation; electronic money institutions exempted pursuant to Directive 2009/110/EC; and small institutions for occupational retirement provision."

[14] See ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification (europa.eu)

[15] Ibid

[16] See Access the Official Journal – EUR-Lex (europa.eu), 25 June 2024

[17] JC 2024-33 – Final report on the draft RTS and ITS on incident reporting (europa.eu)

[18] Article 18 of DORA covers the classification of ICT-related incidents and cyber threats

[19] Article 19 covers reporting of major ICT-related incidents and voluntary notification of significant cyber threats

[20] JC 2024-35 – Final report on RTS on harmonisation of conditions for OVS conduct (europa.eu)

[21] JC 2024 54 – Final report RTS on JET (europa.eu)

[22] JC 2024-29 – Final report on DORA RTS on TLPT (europa.eu)

[23] TIBER-EU is a European Framework for threat intelligence-based ethical red teaming. These tests mimic the tactics, techniques and procedures of real-life attackers based on bespoke threat intelligence. The 'red team' is usually an external cyber security provider, while the attacked firm's cyber defence process is called the 'blue team'.

[24] Information on the blue team's response to each attack step described in the red team test report.

[25] JC 2024-33 – Final report on the draft RTS and ITS on incident reporting (europa.eu)

[26] JC 2024-34 – Final report GL on costs and losses (europa.eu)

[27] JC 2024-36 – Final report on GL on oversight cooperation (europa.eu)

[28] JC 2024-53 – Final report DORA RTS on subcontracting.pdf (europa.eu)

[29] See Implementing DORA – Achieving enhanced digital operational resilience in European financial services – Remarks by Director Gerry Cross at https://www.centralbank.ie/home

[30] The "6-Months to DORA" was organised by the Institute of International Finance and Amazon Web Services and held on 28 June 2024.

[31] dora-checklist-eng (1).pdf

[32] See Launch of a DORA Readiness Survey at https://www.cssf.lu/en

Please contact for further details:

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

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

Kelli O'Brien
United States
Head of Fund Administration
Product
kelli.a.obrien@citi.com
+1 617 859 3468

Ramesh Selva
North & South Asia (ex-Korea)
Head of Trustee & Fiduciary Services
ramesh.selva@citi.com
+65 6657 4142

Sung-Wook Han
Korea
Head of Trustee & Fiduciary Services
sungwook.han@citi.com
+82 22004 2162

Shane Baily
EMEA Head of Fiduciary Services
UK and Europe
shane.baily@citi.com
+353 1 622 6297

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

www.citibank.com/mss

cbs38596 09/24