14 JULY 2023

DRAFT TECHNICAL STANDARDS FOR DORA NOW AVAILABLE

AUTHORS: ANA HADNES BRUDER, OLIVER YAROS, BENJAMIN BECK, LIVIA CREPALDI WOLF

EXECUTIVE SUMMARY

- The EU Digital Operational Resilience Act ("DORA") entered into force in January 16, 2023, setting forth **security requirements for network and information systems** of organizations operating in the financial sector;
- Obligations under DORA are to be further detailed by **Regulatory Technical Standards** ("RTS") and **Implementing Technical Standards** ("ITS"), aimed at **harmonizing requirements** and **facilitating implementation**;
- On June 19, 2023, the European Supervisory Authorities ("ESAs")[1] published the first batch of drafts on RTS and ITS under DORA, providing detail to certain obligations around:
  - **ICT security tools, policies and procedures**;
  - **Policies** on the **use of third-party ICT services** concerning critical or important functions;
  - **Criteria** for **the classification of ICT-related incidents**; and
  - **Register of agreements with third-party ICT service providers**.
- The drafts will be open to **public consultation** until September 11, 2023. The ESAs shall submit these draft technical standards to the European Commission ("Commission") by **January 17, 2024** for adoption by the Commission.
- DORA will apply **from January 17, 2025**, and compliance must consider the content of the RTS and ITS.

BACKGROUND

DORA **enhances security requirements for network and information systems** of organizations operating in the financial sector. Under DORA, ICT stands for information and communication technology. A key notion under DORA is ICT risk, which relates broadly to risks arising in relation to the use of network and information systems.

[1] These include the European Banking Authority ("EBA"), the European Insurance and Occupational Pensions Authority ("EIOPA"), and the European Security and Markets Authority ("ESMA").

DORA applies to a **large range of financial entities**, including credit and payment institutions, electronic money institutions, investment firms, alternative investment funds managers, insurance undertakings, amongst others. It also **directly** applies to companies considered a **critical ICT third-party providers**, as well as **indirectly** to **ICT third-party providers** supplying in-scope entities. DORA creates many obligations for in-scope entities, including in relation to:

- **ICT Risk Management, Testing, and Incident Handling:** in-scope entities will need to implement a series of measures and policies in order to be compliant with DORA, in particular regarding ICT security tools, policies and procedures, cybersecurity governance and asset inventory, business continuity, incident handling, backup and testing policies, trainings, among others;
- **Governance obligations:** in-scope entities will need to have a control function for ICT risk and management bodies will have **direct obligations** with regard to the approval and oversight of the cybersecurity program;
- **ICT Third-Party Risk Management:** building on existing guidance from EBA, ESMA and EIOPA, in-scope entities will be required to review or implement certain key documents and processes, such as a policy on the use of third-party ICT services concerning critical or important functions, a register of contracts with third-party ICT service providers, third-party due diligence, policies or playbooks regarding contractual requirements with third-party ICT service providers and an assessment of ICT concentration risk, among others.

WHAT'S NEW

On June 19, 2023, the European Supervisory Authorities ("ESAs")[2] published the first batch of **drafts on technical standards** under DORA, providing details on certain obligations created by the new regime, including:

OBLIGATION UNDER DORA	SPECIFICATIONS UNDER DRAFT TECHNICAL STANDARDS
ICT Risk Management Under DORA, financial entities are required to enhance, design and implement **ICT security tools, policies and procedures** in line with industry standards.	Draft RTS requires the ICT risk management framework to, among other topics: • Establish measures around netwo**rk security, asset management** security, **data encryption** through cryptography, regular maintenance and **load testing, physical security**, regular awareness **training, controlled** personnel access, and regular **logging** and **reporting**; • **Embed each ICT activity in the risk management framework**, through the establishment of **control measures**, personnel **responsibilities**, and **preventive measures** and procedures to minimize damage in the event of non-compliance; and

[2] These include the European Banking Authority ("EBA"), the European Insurance and Occupational Pensions Authority ("EIOPS"), and the European Security and Markets Authority ("ESMA").

OBLIGATION UNDER DORA	SPECIFICATIONS UNDER DRAFT TECHNICAL STANDARDS
	• Put measures in place to **prevent and manage ICT** incidents, such as **providing logs** of the incident, creating and maintaining **analysis mechanisms** to prevent future similar incidents, and creating an **early warning system**.
ICT Third-Party Risk Management Under DORA, financial entities are required to **manage risks** in connection with providers of ICT-related services. This includes: • **adopting a policy** on the **use of third-party ICT** services concerning critical or important functions; and • establishing a **register** of all ICT-related contractual arrangements	Draft RTS requires the policy on ICT services to, among other topics: • Define a **methodology** for **determining which ICT services support critical or important functions** • **Assign internal responsibilities** around relevant contractual arrangements • Require that ICT services supporting critical or important functions are subject to **independent review** and **included in the entity's audit plan** • **Specify requirements for each main phase of the lifecycle** of the use of ICT services (specifying planning, due diligence, process to select and assess the suitability of providers, implementation, monitoring and management, documentation and record-keeping, **exit strategies and termination processes**) • Identify, prevent and manage actual or potential conflicts of interest • Be **reviewed** and **updated** by the **management body** at least once a year
	Draft ITS proposes a **template** for registering information under different contractual forms, with explanations and instructions for completion.
Incident Handling Under DORA, financial entities are required to **report major ICT-related incidents** to their supervising competent authority.	Draft RTS sets out materiality thresholds for classifying incidents as "**major**". The threshold is met when at least **two primary criteria or one primary criterion and two secondary criteria** are met: • **Primary criteria** include the amount and relevance of clients, financial counterparts and transactions affected by the incident; • **Secondary criteria** include the **reputational and economic impact, duration and geographical spread** of the incident. The criteria proposed are qualitative and binary (i.e. a yes/no answer).

NEXT STEPS

The draft technical standards are open to public consultation until September 11, 2023. The ESAs shall submit these draft technical standards to the Commission by **January 17, 2024** for adoption by the Commission.

Additionally, the ESAS shall propose a second batch of technical standards specifying the content of further obligations under DORA. This second batch shall be submitted to the Commission by **July 17, 2024** and cover the following aspects:

- **Threat-Led Penetration Testing**: competent authorities may identify certain financial institutions as requiring thread-led penetration testing, the requirements of which will be defined in RTS;
- **Content and Timeline of Incident Reporting**: standards shall define the elements to be incorporated in the report and the time limits for the initial notification and follow-up reports;
- **Subcontracting of critical or important functions**: standards shall specify the elements a financial entity needs to assess when subcontracting ICT services supporting critical or important functions.

WHAT BUSINESSES SHOULD BE DOING NOW

The deadlines established in DORA for adoption of relevant standards will leave entities directly and indirectly under scope limited time (one year, at most) to ensure compliance. In-scope entities could benefit from **early compliance efforts**, such as examining processes and policies in place and conducting a gap assessment in view of the requirements established in DORA and the draft technical standards.

Mayer Brown is a leading international law firm positioned to represent the world's major corporations, funds, and financial institutions in their most important and complex transactions and disputes. Please visit www.mayerbrown.com for comprehensive contact information for all our offices. This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein. Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England & Wales), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) and non-legal service providers, which provide consultancy services (collectively, the "Mayer Brown Practices"). The Mayer Brown Practices are established in various jurisdictions and may be a legal person or a partnership. PK Wong & Nair LLC ("PKWN") is the constituent Singapore law practice of our licensed joint law venture in Singapore, Mayer Brown PK Wong & Nair Pte. Ltd. Details of the individual Mayer Brown Practices and PKWN can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown.