kyndryl

Kyndryl and DORA

What is DORA?

The Digital Operational Resilience Act (DORA) is an EU regulation that came into force on January 16, 2023 and will be fully effective on January 17, 2025. DORA will impose uniform requirements for the security of network and information systems of a broad set of entities in the EU financial services industry (FEs) and their respective information and communications technology (ICT) third-party service providers (TSPs).

Prior to DORA, the EU operational resilience and cybersecurity risk management governance model for FEs was based on a disparate collection of national rules, guidelines, and practices that did not empower EU financial supervisors to impose uniform requirements on FEs nor to assess the risks arising from their dependence on TSPs.

DORA attempts to fix these disparities and uneven national regulatory or supervisory approaches. It empowers relevant European supervisory authorities (ESAs)—the European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA), and European Securities and Markets Authority (ESMA)—to develop regulatory technical standards (RTSs) relating to each of the five primary pillars identified below. DORA and its associated RTSs will be enforceable across all 27 EU member states as of January 17, 2025. A TSP that is unable or unwilling to comply with the requirements imposed by DORA will not be eligible to provide ICT services to FEs after that date.

Who is in scope?

DORA establishes uniform requirements relating to the security of networks and ICT systems of FEs and, indirectly, their TSPs. The FEs subject to DORA broadly include 20 different types of entities, ranging from traditional banking, credit, payment, and electronic money institutions, to investment firms, crypto-asset service providers, trading venues, insurance and reinsurance companies, and rating agencies.

"Critical TSPs" are specific ICT TSPs, deemed by the ESAs to be "systemically important" to the EU financial services industry, providers of services to "systemically important" FEs, or providers of "critical or important" services to financial institutions in the EU. Critical TSPs will be subject to heightened regulatory requirements and oversight.

The ESAs will specify more specific criteria for designating a TSP a critical TSP by July 17, 2024. Thereafter, the ESAs will designate each TSP deemed a critical TSP, the ESA that will serve as Lead Overseer (LO) for the critical TSP, and the date on which the LO's direct oversight of the critical TSP will begin.

Five main pillars of DORA

1. **ICT risk management**

- All FEs must implement a detailed ICT risk management framework and strategy, including identification, protection, prevention, recovery and response, leaning, and communication.

2. **ICT-related incident reporting**

- All FEs must monitor and log ICT-related incidents and classify them based on a still-to-be-defined set of criteria
- Major incidents must be reported to relevant national authorities using standardized templates on an initial, intermediate, and final reporting basis.

3. **Digital operational resilience testing**

- All FEs need to implement basic testing requirements
- FEs deemed to be systemically important by competent authorities will be required to implement more advanced testing (for example, threat-led penetration testing).

4. **ICT third-party risk**

- FEs need to devise a strategy to manage ICT third-party risk and identify all contractual arrangements and the specific ICT services provided by their TSPs.
- FEs must have the right to monitor and inspect their TSPs' compliance with DORA requirements.

5. **Information sharing**

- FEs can engage in a voluntary exchange of information and intelligence on cyber threats.

Key features

These are the key features of DORA as we know it today. Teams are working to narrow our focus on how DORA will impact Kyndryl.

- DORA considers the differences between FEs in terms of their size and overall risk profile.
- FEs need to balance their ICT-related needs with their size, nature, scale, and the complexity of their services, activities, and operations. Competent EU authorities will assess and review this approach on a regular basis.
- DORA requires FEs to ensure their contractual arrangements with TSPs are preceded by analyses of the criticality of the services, the necessary supervisory approvals, and possible concentration risks.
- Grounds for termination of contractual arrangements include significant breaches of terms, evidence of weaknesses in an ICT third-party service provider's overall ICT risk management, or circumstances that indicate the inability of the relevant competent authority to supervise.
- Oversight framework includes a proportionate sanctioning regime in case of non-compliance.
- Penalties for non-compliance by critical TSPs (up to 1% average daily worldwide turnover) will be applied daily.

Next steps

As supplements to the text of DORA, The ESAs—in consultation with the European Central Bank, the European Union Agency for Cybersecurity (ENISA), and the European Commission—will publish multiple RTSs ahead of the effective date (January 17, 2025) pursuant to the following timeline:

By January 17, 2024 the ESAs will publish RTSs on these topics:

- Risk-management tools, methods, processes, and policies
- ICT management framework
- Classification of ICT-related incidents and cyber threats
- Management of ICT third-party risks

By July 17, 2024 the ESAs will publish RTSs on these topics:

- Reporting contents and templates
- Advanced testing of ICT tools, systems, and processes, based on threat-led penetration testing
- Key contractual provisions
- Designations for critical TSPs
- Ongoing oversight

The ESAs will seek input and organize stakeholder consultations on these topics between May and September 2023, and between November 2023 and February 2024, respectively.

For more information

Please contact your Kyndryl representative for more information and visit our Security and Resiliency webpage to learn more about our offerings.

kyndryl