RocaJunyent Informs

Department of Data Protection, New Technologies, and Cybersecurity
30 May 2023

The DORA Regulation updates and manages information and communication technology ("ICT") risk requirements across the EU financial sector in a homogeneous way, so that it is able to maintain its resilience in the event of an operational disruption.

When will it be applicable?

The Regulation entered into force on 16 January 2023 and will apply from 17 January 2025.

What is the scope?

DORA will have a very broad application and will cover authorised European financial institutions (such as credit institutions, investment firms, payment institutions, data reporting services, insurance intermediaries, credit rating agencies, etc.) as well as third-party ICT service providers (Art. 2 DORA).

At the same time, the Regulation recognises that there are significant differences between financial institutions in terms of size, business profiles or in relation to their exposure to risk, and establishes a principle of proportionality, so that it imposes stricter obligations on larger institutions (Art. 4 DORA).

What does it imply to the organization of the entity?

The full responsibility of the management body for the management of the ICT risk of the financial institution will be a general principle that will result in a set of specific requirements, such as the assignment of clear tasks and responsibilities for all ICT-related functions, control, ICT training, etc. (Art. 5 DORA).

Institutions should have a governance framework in place to ensure the effective management of ICT risks and appoint a Chief Information Security Officer ("CISO"). In this way, it transfers the focus of information security management systems that were already defining standards such as UNE-ISO 27001 for those companies that opted for certification.

How is ICT risk management foreseen?

Financial institutions must have a complete and robust ICT risk management framework (art.6-16 DORA), covering:

- **Identification** of business functions related to ICT and information assets;
- **Protection and prevention** by designing and implementing ICT security strategies, procedures, policies and tools;
- **Detection** of anomalous ICT-related activities;
- **Response and recovery**, recording incidents, ensuring business continuity, implementing containment and crisis management plans and periodically testing its business continuity policy and recovery plan.
- **Reduce recovery times** by restoring ICT systems after an incident with minimal downtime and limited disruption;
- **Learning and evolution** (both in terms of skills and resources and staff).

What is digital operational resilience testing?

These tests consist of checking the state of preparedness of the systems of financial institutions in the face of ICT-related incidents. Entities will be obliged (art.24-27 DORA) to carry out these tests with essential ICT systems and applications at least once a year. Two different types of tests are contemplated according to the size and importance of the entity, basic and advanced.

Will incidents need to be reported?

Institutions shall record incidents and classify them according to the materiality criteria set out in DORA (Art.17-23 DORA) and shall only report to the competent authorities ICT-related incidents that are considered to be serious. Financial institutions should submit initial (first day), intermediate (first week) and final (first month) reports and inform their users and customers when the incident has or is likely to have an impact on their financial interests.

These reporting obligations should be coordinated with other reporting obligations under other standards. The regulation foresees the possibility for European supervisors to develop a system of standardization and centralization of incidents, through the creation of a Hub, although the criteria are still to be defined.

What does DORA mean for ICT providers?

ICT providers (art.28.44 DORA) are companies that offer digital and data services, such as cloud services, software and analytics and data centers.

DORA is based on the general principle that provider-related risks should be integrated into the ICT risk management framework of each financial institution, so they will have to carry out constant monitoring of their agreements with them. In addition:

- Thus, "critical" providers may be designated, depending on the financial institutions that depend on their services, which will be supervised by one of the competent authorities (EBA, EIOPA and ESMA). They may request information and carry out general investigations and on-site inspections. In case of non-compliance, the authorities may impose periodic penalty payments on suppliers.

- Companies wishing to engage ICT providers established in a third country and designated as essential may only do so if they have established a subsidiary in the EU in the last 12 months prior to the designation (Art.31.12).