DORA – what do you need to know?

SORAINEN

What is DORA?

DORA (Digital Operational Resilience Act) is an EU regulation that aims to strengthen the resilience of the financial sector's digital operations by ensuring effective information and communication technology (ICT) risk management and incident monitoring, with consistent requirements across EU Member States. DORA requirements apply from 17 January 2025.

Who is covered by DORA?

The requirements apply to financial sector entities listed in Article 2 of DORA, including banks, insurance companies, electronic money and payment institutions and investment firms. Individual DORA requirements vary depending on the size of the financial sector entity.

What are the implications of non-compliance?

- A lack of preparation leaves organisation vulnerable to cyber-attacks, which can result in financial losses, loss of competitiveness and threats to business continuity.
- The Bank of Lithuania, in its supervisory role over the financial market, has the authority to impose various sanctions, including fines.
- Reputational impact and loss of customer confidence.
- Direct financial losses.
- Loss of income due to disruption of ongoing operations.
- Costs associated with restoration and repair of affected IT systems.
- Loss and recovery of information necessary for the operation.
- Finally, it is important to consider the damage to other organisations with which you cooperate in the course of provision of your services.

What are the requirements under DORA?

5 key pillars of DORA requirements

1

Incident management

DORA requires financial sector entities to properly manage and report ICT-related incidents to the relevant authorities.

2

Digital operational resilience testing

Financial sector entities are required to carry out regular system testing to ensure resilience to disruptions and ICT-related risks.

3

Risk management

DORA emphasises structured risk management, including proactive monitoring, threat management and the integration of ICT system safeguards.

4

ICT service provider risk management

Strict third-party risk management policies are required, including thorough screening of service providers, their register and appropriate contractual provisions.

5

Information sharing

DORA promotes the exchange of information on cyber threats and best market practices between financial sector entities.

How to ensure compliance with DORA?

1 **Define the scope** ✓
Under Article 2 of DORA, assess whether your organisation falls within its scope. This requires an assessment of factors such as the size of your company and the type of services you offer.

2 **GAP analysis** ○
Take a close look at your current ICT systems and compare them with the requirements of DORA.

3 **GAP remediation plan** ○
Once you have identified the gaps, prioritise your actions in terms of risk and resources to make sure your plan is realistic and achievable.

4 **Key ICT service providers** ○
If you work with third-party ICT service providers, make sure they are fully compliant with DORA requirements.

5 **Threat-led penetration testing** ○
Implement testing using approved systems.

6 **Incident response plan** ○
Establish a clear process for managing ICT incidents, including procedures for identifying, tracking and classifying problems.

7 **Continuous ICT monitoring** ○
Regularly monitor and assess the risks of ICT systems, and keep an up-to-date inventory of ICT systems.

8 **Management responsibilities** ○
Ensure that the organisation's security policy is maintained and digital resilience strategies are adopted.

9 **Documentation practices** ○
Record everything related to your compliance - risk assessments, incident reports, testing results.

10 **Training and awareness** ○
Develop appropriate training programmes to raise your employees' awareness of cyber security risks.

How can we help?

As DORA implementation requires more than just legal expertise, by working with experienced cybersecurity experts, we can help clients with:

- Assessing the specific requirements applicable to an organisation
- Compliance GAP assessment
- Network and information systems risk assessment
- Preparation of documentation
- Implementation of supply chain security requirements
- Managing cyber incidents and reporting to authorities
- Penetration testing
- Training for managers and employees

Contacts

Irma Kunickė
Counsel

M. +370 66 377 166
T. +370 52 685 040
irma.kirklyte@sorainen.com

Stasys Drazdauskas
Counsel

M. +370 61 122 910
T. +370 52 685 040
stasys.drazdauskas@sorainen.com

Raminta Matulytė
Associate

M. +370 61 062 865
T. +370 52 685 040
raminta.matulyte@sorainen.com

Sidas Sokolovas
Senior Associate

M. +370 62 304 665
T. +370 52 685 040
sidas.sokolovas@sorainen.com