Arendt by your side for every step of DORA implementation

Why the Digital Operational Resilience Act (DORA)?

The EU's DORA regulation, in force as from 16 January 2023, creates a unified regulatory framework for digital operational resilience which requires all types of EU financial entities to ensure they can withstand, respond to, and recover from any ICT-related threats.

DORA was created as a response to the increased risks arising from the EU financial services sector's reliance on ICT, as well as the lack of harmonised EU-level rules on digital operational resilience and the resulting fragmented and inconsistent rules at EU Member State level. In line with wider EU efforts to strengthen cybersecurity and address broader operational risks, DORA aims to harmonise and streamline the handling of ICT risk management by financial entities.

! On 5 January 2024, the CSSF released a circular on ICT-related incident reporting frameworks, which outlines prior to DORA certain requirements that must be complied with under both this circular and DORA.

Who is impacted by DORA?

>> **Most financial companies**, including credit institutions, payment and electronic money institutions, investment firms, insurance and reinsurance undertakings, most AIFMs and management companies

>> **ICT third-party providers**, including cloud service providers (CSP)

>> **For microenterprises**, specific provisions apply

The numerous exceptions, depending on the provision, make a number of requirements complex to understand; therefore, each affected company must conduct a careful analysis to clarify the applicable provisions, based on its specific profile.

What are the main requirements under DORA applicable to in-scope entities?

1 - ICT RISK MANAGEMENT	□ Put in place the required governance and control framework to ensure prudent ICT risk management, based on the management body's accountability and the proportionality principle □ Use and maintain systems, protocols and tools allowing sufficient reliability, capacity and resilience (Identify, Protect, Detect, Respond, Backup & Recover)
2 - ICT-RELATED INCIDENT MANAGEMENT, CLASSIFICATION & REPORTING	□ Establish a compliant process to detect, manage, notify and record any ICT-related incident □ Develop the required classification criteria by criticality of the incident □ Prepare for reporting of major ICT-related incidents, including client notification protocol and management of outsourcing of reporting obligations as may be relevant
3 - DIGITAL OPERATIONAL RESILIENCE TESTING	□ Establish and maintain a sound and comprehensive testing programme, follow a risk-based approach and use independent testers □ Comply with relevant ICT tools and systems testing terms □ For affected companies, apply threat-led penetration testing at the relevant frequency
4 - MANAGEMENT OF ICT THIRD-PARTY RISK	□ Manage ICT third-party risk as part of ICT risk, regularly review the ICT third-party risk strategy □ For technically complex ICT services, ensure that internal and external auditors possess appropriate skills and knowledge □ Designate and specifically manage critical ICT third-party service providers
5 - INFORMATION-SHARING ARRANGEMENTS	□ Develop information-sharing arrangements with other financial entities around cyber threats

Arendt by your side for every step of DORA implementation

Timeline and important milestones

DORA ENTERS INTO FORCE
16 January 2023

RTS / ITS
17 January 2024

RTS / ITS / DAs
17 July 2024

DATE OF APPLICATION
17 January 2025

2023 | 2024 | 2025

RTS: Regulatory Technical Standard | ITS: Implementing Technical Standard | DA: Delegated Act

How can Arendt help you?

APPLICABILITY ANALYSIS AND SCOPE

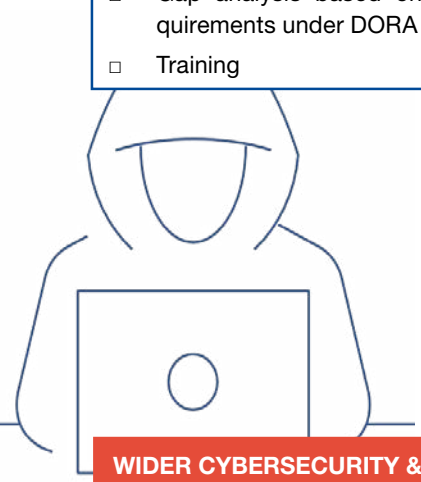
- Applicability analysis for each client/details of applicability (many DORA provisions are intended for certain entity profiles only)
- Gap analysis based on new requirements under DORA
- Training

DORA REMEDIATION SERVICES

- Drafting/review of ICT strategy, policies and procedures, including for compliance with the CSSF Circular on ICT-related incident reporting framework
- Support with preliminary mapping and critical analyses of business functions and ICT assets
- Review of due diligence questionnaires
- Drafting the required registers
- Contract alignment
- ICT training

AD HOC SUPPORT

- Managing the impacts of ICT incident events on an ad hoc basis
- Incident management processes
- Security analysis of ICT third-party providers
- Testing programmes



WIDER CYBERSECURITY & INFORMATION PROTECTION SUPPORT

Arendt's Cybersecurity & Information Protection Team provides comprehensive support from a legal, regulatory, financial crime and operational perspective, assisting you across the cybersecurity & information protection lifecycle. Beyond regulatory challenges such as DORA, our team can also provide assistance with: crisis management & communication, training, 360 risk assessment and response-readiness, asset identification and search, forensic investigation, extortion & ransom management, litigation and claims handling, amongst others.

contact us: cybersecurity@arendt.com

arendt.com