www.pwc.lu/dora

EU Digital Operational Resilience Act - Business, operational, IT and compliance implications to be considered

As of January 2025 around 22,000 EU regulated financial entities (e.g. banks, insurance companies, management companies, AIFMs, PSF (expected)) are required to comply with uniform regulatory standards that have two main objectives:

- To require in-scope entities to build, assure and review their operational integrity to ensure the continued provision of their financial services and their quality including throughout disruptions.
- To limit the risk of contagion within the EU financial system by prescribing a harmonised minimum standard of digital operational resilience.

DORA is an all-encompassing regulation that will challenge the setup of every organisation that is directly in scope as well as entities that might be indirectly affected (e.g. service providers) to their core.

Your challenges

- **Understanding what DORA means for your current business model and operational setup and how your service and operating model may be required to change - or - if and how you can safeguard the status quo.**
- **Understanding what elements of DORA are currently (not or partially) embedded in your organisation and across your value chain.**
- **Understanding how DORA requirements can be implemented efficiently within your organisation (and across the group) and how to seize opportunities that DORA offers.**
- **Understanding what elements required by DORA can be efficiently outsourced to a third party provider.**

Group settings render these challenges more complex. Group settings with Non-EU dependencies add another layer of sophistication to the DORA requirements.

pwc

DORA pillars

- Governance - New responsibilities at entity level include, amongst others, the ultimate responsibility for managing the entity's ICT risk as well as the establishment of policies allowing for high standards regarding data management.
- ICT risk management - proper identification of risks related to business functions, information and ICT assets, and related dependencies, with a special focus on “critical or important functions”.
- ICT incident reporting - proper identification of ICT incidents and significant cyber threats, their remediation and communication.
- Digital operational resilience testing – elaboration and performance of a set of tests that will cover critical ICT systems and applications.
- ICT third party risk management - new contractual provisions incl. right of on-site visits, third party provider strategy, substantive ongoing inventory duties at entity and consolidated level (group).
- Information and intelligence sharing – voluntary exchange of information between financial entities in a trusted community.

Entities in scope

- Credit institutions
- Payment institutions
- E-money institutions
- Investment firms
- Crypto-assets service providers
- Central securities depositories
- Central counterparties
- Trade repositories
- Securitisations repositories
- Managers of AIFs
- Management companies
- Insurance and reinsurance
- Institutions for occupational retirement provision
- ICT third-party service providers
- PSF (expected)

Our services

Understanding the implications on your business and service model.

Readiness assessment of your organisation with DORA requirements.

Implementation support (e.g. (i) mapping of processes, information assets, ICT assets, (ii) coherent ICT risk taxonomy, (iii) third party management, (iv) resilience testing incl. pen-tests and TIBER-LU framework etc.)

Managed services:
- Third party provider management incl. risks;
- CISO as a service;
- Resilience testing;
- Incident reporting;
- ICT and operational risk support.

DORA trust attestation
- IT attestation/controls report based on implemented processes.

Your benefits

- End-to-end thinking across the value chain and different entities.
- Business focused implementation advice.
- Managed services limiting impact on your operating model and ensuring compliance.

For more information on DORA, please contact:

Michael Horvath
Advisory Partner, Regulatory & Change Management
PwC Luxembourg
+352 621 333 612
michael.h.horvath@pwc.lu

Patrice Witz
Advisory Partner, Technology Partner and Digital Leader
PwC Luxembourg
+352 621 333 533
patrice.witz@pwc.lu

Olivier Carré
Deputy Managing Partner, Technology & Transformation Leader
PwC Luxembourg
+352 621 334 174
olivier.carre@pwc.lu

pwc