Digital Operational Resilience Act (DORA)

What it means for you and considerations for next steps

What is DORA?

The Digital Operational Resilience Act (DORA or "the Act"), forms part of the European Commission's digital finance package, which aims to strengthen the resilience of the EU financial sector. Published in the Official Journal of the European Union (OJEU) on 27 December 2022, DORA entered into force on 16 January 2023. The Act provides consistent rules addressing the digital operational resilience needs of all regulated financial entities and establishes an oversight framework for critical ICT third-party providers (CCTPs). Firms have 24 months to implement the requirements and comply. The Act will apply from 17 January 2025.

Why was DORA introduced?

DORA aims to mitigate digital transformation risk though common EU-wide rules on operational resilience. It has been introduced to:

1. Mitigate risk posed by growing vulnerabilities, due to the increasing interconnectivity of the financial sector
2. Address the shift in risk profile as a result of the increase in financial services digital adoption
3. Acknowledge and address the third-party reliance underpinning the stability of the financial sector
4. Adopt a single, consistent supervisory approach to operational resilience across the single market

Who does DORA impact?

DORA is applicable to regulated financial institutions including traditional institutions such as credit institutions, payment institutions and insurers, as well as crypto-asset service providers (CASPs), crypto-asset issuers and electronic money institutions (EMIs). Financial information managers, data information service providers, credit rating agencies, legal auditors and audit firms, and CCTPs (i.e., digital and data service providers, including cloud service providers, software, data analytics services, and data centers), are also in scope.

While the rules cover all financial entities, their applicability will depend on the size of the entity, its activity and the overall risk to which it is subjected. Micro-enterprises will benefit from this flexibility and will be subject to proportionate application of requirements on ICT risk management, digital resilience testing, reporting of major ICT related incidents and oversight of critical CCTPs.

Four focus areas to familiarize yourself with

ICT risk management framework and governance

This focus largely builds on the European Banking Authority's (EBA) ICT and Security Risk guidelines, defining how to manage risks through each stage of their lifecycle, emphasizing the role of senior management and expanding the requirements to include a digital resilience strategy. There are also additional requirements around disaster recovery, communications and crisis management. Requirements to learn and evolve both from external events as well as the firm's own ICT incidents are set out.

Management of ICT third-party risk

The existing EBA outsourcing requirements are broadened, requiring firms to expand their register of providers to include all contractual arrangements rather than just those classified as outsourcing. DORA also requires firms to have a strategy on ICT third-party risk. It sets out more detailed guidance around the content of exit plans and substitutability assessments, and testing thereof. The regulations also look to limit the use of third parties outside of the EU.

Incident reporting and information sharing

ICT related incidents are extended to sectors not previously covered. The multitude of reporting requirements imposed on a firm are addressed, attempting to streamline reporting with common templates, timeframes and a single point of reporting. Additionally, the guidelines encourage collaboration among trusted communities of other financial entities on cyber threat information and intelligence.

Operational resilience testing

It is suggested that firms establish testing programs proportionate to their size, business and risk profiles. This includes a range of assessments, tests, methodologies, practices and tools. Ultimately, testing should be risk-based – considering the risk horizon, as well as firm-specific risks and the criticality of ICT resources and the services that they support. Testing should consider the principle of applying "extreme scenarios" where relevant and involve participation of contracted third parties.

For more details on DORA, read our dedicated article here

Next steps for you and your business

Financial institutions currently under the European Commission's supervisory model and scope should assess if their current state meets the expanded regulation and plan accordingly to respond across the themes. There are six pillars to pay attention to:

Governance
Assess existing ICT risk governance (for regulated entities and inter-entity) to identify gaps in direction, evaluation or monitoring of ICT risk topics.

ICT risk framework
Assess existing ICT risk strategy, policies, procedures and tools. Consider roles and responsibilities skills in IT and Risk.

Incident risk reporting
Review incident identification, classification and reporting protocols against leading practice (including existing PSD2 expectations) to identify if investment in process/tooling is needed.

Resilience testing
Assess the scope of threat-led penetration testing (akin to CBEST and TIBER), contributing to DORA testing expectations.

"Critical" ICT third-party status
Assess the services received from third-party service providers to identify any additional required governance and oversight.

Information sharing
Assess the capabilities for voluntary exchange among financial entities regarding cyber threat intelligence in trusted forums.

DORA voted in the European Parliament	DORA came into force	Publication of RTS, ITS and DA	Expected enforcement of DORA
November 2022	**16 January 2023**	**Q1/Q2 2024**	**17 January 2025**

How EY can help

As part of strategy consulting, we support various actors in the financial industry in designing, implementing or assessing the effectiveness and efficiency of ICT risk programs, compliance positions and how risks are managed now and going forward (resilience). EY has also developed Third Party Security Risk Management (TPRM) solutions providing a support function for management bodies to identify, evaluate, monitor and manage the risks associated with third parties and contracts. Some of our services are outlined below.

DORA readiness current state assessments & multi-year roadmap

We perform assessments by leveraging existing mapping information (such as business impact analysis, privacy data flow mapping, technology asset inventories) that exist within your organization.

Resilience testing & attack simulation

We can assess your organization's resilience through the testing of your detection and response capabilities by staging simulated cyberattacks (red teaming, TIBER-LU, etc.).

Incident response services

We help your organization to be ready for a breach and mitigate the impact of an eventual security incident. To that extent, we assist you in building, maintaining and testing your incident response plan.

Third party profiling, and risk & controls assessments

We perform service risk profiling and global onsite and remote-control assessment execution across all risk domains (e.g., resiliency, cyber, financial health and regulatory compliance).

Why EY?

We are the only audit and consulting firm fully dedicated to financial services in Luxembourg. As such, we have an exhaustive, sector-spanning view of industry risks and regulatory developments. By providing local insights, exceptional client service and representing your interests in legislative and standard-setting processes, we can help you navigate the complexities of your most important challenges and markets. This allows you to stay focused on the future of financial services - one that is stronger, fairer and more sustainable. We have a track record of delivering operational resilience transformation. We continue to evolve our thinking and delivery approaches as the industry regulatory environment, and nature of resilience challenges, evolve.

We have developed tools and enablers to ensure a successful execution of your DORA compliance journey with the required quality. In Luxembourg, we currently have a team of over 50 technology consulting professionals and cybersecurity experts, spanning 20 nationalities. Our local team benefits from the connectedness of the global EY network. With over 12,400 technology consulting professionals across the world, our Luxembourg team is well-positioned to help clients with an international footprint, who have set up shop in Luxembourg and the rest of Europe.

50+

Technology consulting professionals dedicated to DORA and cybersecurity in Luxembourg

12,400

Technology consulting professionals across the world

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

ey.com/lu

> “We help you build operational resilience and trust while navigating through increasing regulations.
>
> Karim Bouaissi

> “Cyber resilience requires a constant mindset, not just an occasional plan. The real question is not if a cyberattack will occur, but rather, are we truly prepared to respond to it when it inevitably happens.
>
> Guillaume Carballo

Contacts

Karim Bouaissi
EY Luxembourg Consulting Technology Risk Partner
+352 42 124 8779
Karim.Bouaissi@lu.ey.com

Guillaume Carballo
EY Luxembourg Partner, Cybersecurity Leader
+352 42 124 7855
Guillaume.Carballo@lu.ey.com