MITRATECH | Governance, Risk & Compliance

TOP 10 Frequently Asked Questions About the Digital Operational Resilience Act (DORA)

Your Essential Roadmap to DORA Compliance and Resilience

DORA, or the Digital Operational Resilience Act, is an EU regulation designed to ensure that financial institutions can withstand, respond to, and recover from all types of ICT-related disruptions and threats.

This FAQ guide addresses common questions about DORA, helping organizations understand its scope, requirements, and strategies to navigate the new regulatory landscape effectively and meet compliance deadlines.

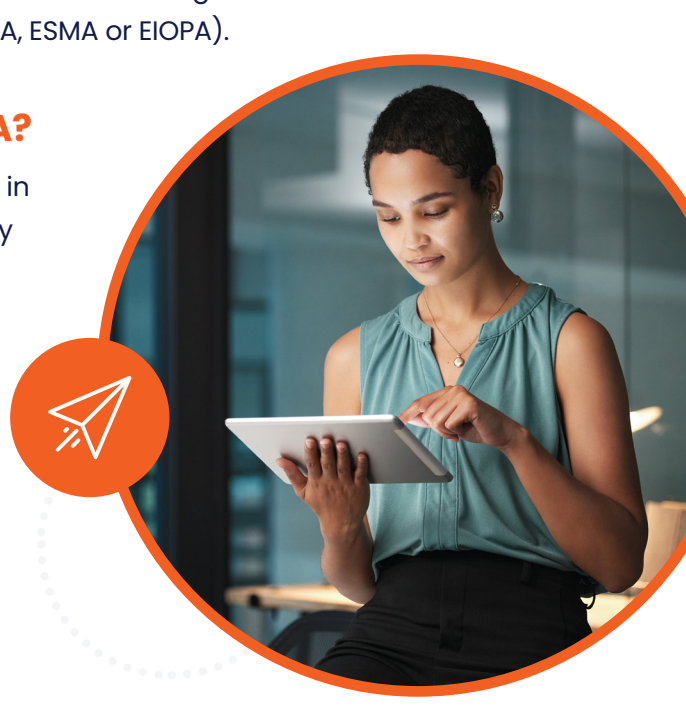
1. Which organizations are affected by DORA?

The scope of DORA covers a wide range of entities within the EU's financial system. This includes banks, investment firms, insurance companies, financial market infrastructures like stock exchanges and clearinghouses, and critical third-party IT service providers, including cloud services.

Additionally, critical third-party ICT providers are also regulated under the regulation. Each critical ICT service provider will be designated a Lead Overseer (either EBA, ESMA or EIOPA).

2. What are the main requirements of DORA?

The key objective of DORA is to improve operational resilience in financial services institutions and enhance business continuity practices in the event of a significant business disruption.



The regulatory framework touches on five main areas:

1. ICT Risk Management
2. ICT Incident Management & Reporting
3. Digital Operational Resilience Testing
4. ICT Third-Party Risk Management
5. Information & Intelligence Sharing

3. When does DORA come into full effect?

DORA requirements became enforceable 24 months after their entry into force on January 16, 2023. While financial entities are expected to comply with DORA by January 17, 2025, several rounds of RTS drafts have already been released, with the final draft expected in December 2024.

4. What are the reporting requirements for ICT-related incidents?

Financial services institutions already must collect data on ICT incidents, report major issues to the authorities and act on supervisory feedback. Under DORA, they must extend these incidents within critical third-parties.

These institutions are required to have a streamlined process to log/classify all ICT incidents and determine major issues. Reporting of major incidents needs to be harmonized through standard templates. Centralization of the reporting process might be explored by establishing a single EU hub for reporting of major incident.

5. How does DORA address third-party risk management?

DORA mandates a comprehensive process for assessing the security measures of third-party vendors and ensuring they also meet compliance requirements. Organizations must assess and manage the operational resilience of these service providers. Contracts with third-party vendors should include specific security and compliance obligations and be regularly reviewed and updated to address evolving risks.

DORA also requires ongoing monitoring mechanisms and periodic audits to ensure vendors comply with these contractual obligations. Additionally, it defines procedures for coordinating incident responses for both the organizations and their vendors.

6. Will DORA affect existing ICT risk management standards?

The EU's new regulation DORA will broadly influence how financial entities improve ICT governance, manage ICT risks, disclose incidents, and strengthen their resilience. DORA will complement and reinforce existing standards and regulations (like ESA + ENISA), requiring organizations to integrate its requirements into their current risk management practices.

7. How does DORA impact cross-border financial services?

DORA aims to create a harmonized framework across the EU, facilitating better coordination and consistency in managing ICT risks for cross-border financial services. As such, Information & Intelligence Sharing Arrangements is highlighted as a domain under DORA where organizations will need to collaborate with other financial services institutions to establish information and intelligence to address evolving cyber threats and industry needs.

8. What are the penalties for non-compliance with DORA?

Penalties can include fines, sanctions, or other enforcement actions by regulatory authorities depending on the severity of non-compliance. Non-compliant financial institutions may be fined up to one percent of their average daily worldwide turnover in the preceding fiscal year.

9. How can organizations prepare for DORA compliance?

As we approach January 17, 2025 — the compliance deadline for DORA — it's essential for financial entities to understand its requirements and prepare accordingly.

But here's the catch: For the first time in history, organizations will only have one month's notice to be fully compliant with new DORA regulation updates following its final release in December. Luckily, teams can start proactively mapping RTS drafts now, leaving the last 30 days for any needed updates or adjustments.

Key Dates to have top of mind for your organization:

December 2024: Final DORA release

January 17, 2025: Impacted companies must have DORA implemented, be able to evidence full compliance, and be able to show continuous improvement.

10. What resources are available to help organizations comply with DORA?

Few platforms on the market have added RTS draft content directly into their platforms to help you start proactively working towards DORA compliance. Mitratech Alyne is purpose-built and hand-curated to help you start today. No need for a rip-and-replace approach or huge overhaul, either. Alyne seamlessly integrates with your existing infrastructure, tools, and technology, acting as a DORA expert to help you understand and map the final draft RTS requirements and efficiently consolidate all necessary data (including that required by the EBA/ESA templates) into the Register of Information ahead of the January 2025 implementation date.

This unique offering gives your team the opportunity to start proactively mapping RTS drafts now, and the peace of mind that you can easily implement any needed updates in those last 30 days.

Guarantee Your DORA Compliance Without a Sweat

When the regulation is eventually finalized (December), Mitratech Alyne will automatically adapt, quickly identify gaps and auto-create actions — all of which would otherwise be overly complicated (and costly) to do from spreadsheets.

Alyne implementation can take 4-6 weeks, so the time is now to start working towards your DORA compliance. Get in touch with our team and take the first step with ease to getting your organization compliant.

Get in Touch ▶

Learn more: info@mitratech.com | mitratech.com

MITRATECH