https://www.bdo.ie/en-gb/insights/2024/dora-understanding-and-preparing-for-the-digital-operational-resilience-act

DORA: Understanding and Preparing for the Digital Operational Resilience Act

18 July 2024

Understand the Digital Operational Resilience Act (DORA) and its impact on financial institutions and ICT service providers. Learn key timelines, requirements, and practical steps to meet the January 2025 compliance deadline. Essential reading for compliance officers, IT managers, and executives to enhance digital resilience and meet regulatory standards.

As the financial landscape becomes increasingly digital, the resilience of financial institutions' digital infrastructures is critical. The European Union's Digital Operational Resilience Act (DORA) aims to ensure that the financial sector can withstand, respond to, and recover from all types of ICT-related disruptions and threats. This comprehensive regulation covers a broad range of entities and imposes stringent requirements to enhance digital operational resilience. Here's what you need to know to navigate DORA with confidence.

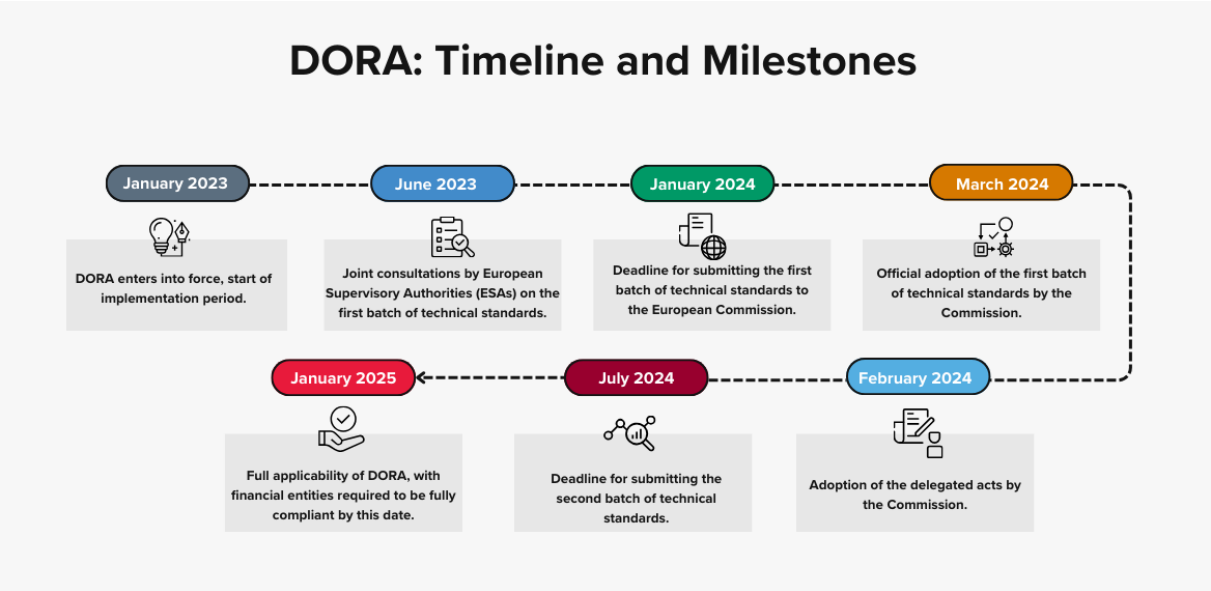
DORA: Overview

Adopted by the European Union Council, DORA aims to bolster the cybersecurity and operational resilience of financial entities and ICT third-party service providers. Recognising that cyberattacks cannot be entirely prevented, the regulation focuses on mitigating their impact on financial stability through robust ICT risk management and resilience measures. By doing so, DORA seeks to protect the integrity of financial services across Europe.

Empty heading

Key Timelines and Implementation Milestones

DORA's implementation is structured over several key milestones to ensure a smooth transition and compliance by January 2025:



In anticipation of the January 2025 deadline, new technical standards and further clarifications are expected, providing detailed guidance on compliance requirements. This upcoming addition will offer clarity on specific technical standards and protocols, ensuring that financial entities are well-prepared to meet DORA's stringent requirements. This addition to the regulatory framework will be crucial for organisations aiming to align their operational resilience strategies with DORA's mandates.

Entities Subject to DORA

DORA applies to a wide array of financial entities and ICT third-party service providers, including but not limited to:

- **Financial Entities**: Banks, credit institutions, payment institutions, electronic money institutions, investment firms, insurance and reinsurance undertakings, crypto-asset service providers, and more.
- **ICT Third-Party Service Providers**: Providers of cloud computing services, software, data analytics, and data centres.

These entities must enhance their collaboration to meet DORA's requirements and ensure the resilience of their digital infrastructure.

Core Requirements of DORA

DORA is structured around five key pillars, each with specific requirements:

1. ICT Risk Management (Articles 5 - 16)

- Establish a comprehensive ICt risk management framework covering identification, protection, detection, response, and recovery processes.
- Ensure the governance framwork is robust, with accountability resting on senior management.

Practical Insight: Regularly update risk management frameworks to adapt to emerging threats and technological advancements.

2. ICT-Related Incident Management, Classification, and Reporting (Articles 17 - 23)

- Standardise incident classification and reporting of major ICT-related incidents.
- Implement compulsory reporting menchanisms and anonymised EU-wide incident reports.

Practical Insight: Develop a streamlined incident reporting process that integrates with existing crisis management protocols to ensure timely and accurate reporting.

3. Digital Operational Resilience Testing (Articles 24 - 27)

- Conduct regular resilience testing, including large-scale threat-led penetration tests every three years by independent testers.

Practical Insight: Schedule periodic internal and external audits to verify the effectiveness of resilience measures and make necessary adjustments based on test outcomes.

4. Managing ICT Third-Party Risk (Articles 28 - 44)

- Develop and maintain a detailed register of information on all contractual arrangements with ICT third-party providers.
- Implement guidelines for pre-contract assessments, contract contents, termination processes, and stressed exit plans.

Practical Insight: Establish clear communication channels and protocols with third-party providers to ensure rapid response to any disruptions.

5. Information Sharing Arrangements (Article 45)

- Encourage financial entities to share threat intelligence and information to enhance collective resilience.

Practical Insight: Participate in industry forums and threat intelligence networks to stay informed about the latest cyber threats and mitigation strategies.

Preparing for Compliance

Achieving compliance with DORA by the January 2025 deadline is challenging but essential. BDO recommends a phased approach to compliance, including:

1. **Gap Analysis**
    - Conduct a thorough gap analysis to identify areas where current practices fall short of DORA requirements. This involves evaluating existing ICT risk management frameworks, incident management processes, and third-party risk management protocols.
2. **Develop a Detailed Implementation Plan**
    - Create a comprehensive plan that outlines specific actions, timelines, and responsibilities for achieving compliance. This plan should address all five pillars of DORA and ensure alignment with upcoming technical standards.
3. **Enhance ICT Risk Management**
    - Update and strengthen ICT risk management frameworks to ensure they cover all necessary aspects, including identification, protection, detection, response, and recovery. Ensure that senior management is fully engaged and accountable.
4. **Incident Reporting and Management**
    - Standardise incident reporting procedures and ensure they align with DORA's requirements. Implement systems for real-time monitoring and reporting of ICT-related incidents and establish clear protocols for escalation and resolution.
5. **Conduct Regular Testing**
    - Implement a schedule for regular resilience testing, including threat-led penetration tests. Ensure that these tests are conducted by independent parties and that findings are used to enhance overall resilience.
6. **Strengthen Third-Party Risk Management**
    - Develop robust third-party risk management practices, including comprehensive assessments before contracting, clear contract terms, and exit strategies. Maintain an up-to-date register of all third-party ICT providers and their compliance status.
7. **Foster Information Sharing**
    - Encourage participation in information-sharing initiatives to stay informed about the latest threats and best practices. Collaborate with industry peers and regulatory bodies to enhance collective resilience.

Penalties for Non-Compliance

Failure to comply with DORA can result in significant penalties. National competent authorities will oversee compliance and can impose fines, including periodic payments of up to 1% of the average daily global turnover of the preceding business year for up to six months until compliance is achieved.

BDO's Support for DORA Compliance

BDO offers expert guidance and comprehensive support to help financial entities achieve DORA compliance. Our services include:

- **Risk Assessments and Gap Analysis**: Our team can support you in identifying potential threats and vulnerabilities and developing mitigation plans.
- **Incident Management and Business Continuity Plans**: We help your organisation effectively respond to major incidents.
- **Cybersecurity Services**: We carry out penetration testing, vulnerability assessments, and incident response planning to ensure your organisation is protected and prepared.
- **Training and Education**: Our experts are happy to help your employees understand and comply with DORA requirements.

Navigating DORA can be complex, but with the right preparation and support, financial entities can enhance their digital operational resilience and secure their operations against potential threats. As the year progresses, additional guidance is anticipated following the dry-run exercises by the European Supervisory Authorities (ESAs) and competent authorities. With the January 2025 compliance deadline rapidly approaching, financial service providers must begin their preparation now. With a tight timeline for compliance, prompt and strategic planning will be crucial to achieving full adherence to DORA's requirements.

References:

Regulation - 2022/2554 - EN - DORA - EUR - Lex (europa.eu)
Digital Operational Resilience Act - EIOPA
BDO Malta - DORA - Brochure (pdf)
Digital Operational Resilience Act (DORA) - Central Bank of Ireland
New draft technical standards provide useful guidance for DORA compliance projects - Arthur Cox
DORA Spotlight: Practical insights on the second batch of draft technical standards - Arthur Cox
Preparation for DORA application - European Banking Authority