SOPHOS

Sophos Guidance on the Digital Operational Resilience Act (DORA)

A Sophos Whitepaper. April 2024

About DORA

The Digital Operational Resilience Act (Regulation (EU) 2022/2554) ("DORA" or the "Act") is a European Union regulation intended to ensure the digital resilience of financial entities[1] in the EU against Information Communication Technologies (ICT) - related incidents and operational disruptions. The European Commission completed DORA on 16 January 2023. Its requirements become effective and apply on 17 January 2025.

Scope of DORA

DORA applies to all EU "financial entities," including banks, investment firms, credit institutions, insurance companies, crowdfunding platforms, as well as critical third parties offering ICT-related services to financial institutions such as software vendors, cloud service providers and data centers, data analytics providers, and more. Article 2 of (EU) 2022/2554 identifies the following financial entities covered by the Act.[2]

LIST OF FINANCIAL ENTITIES COVERED BY THE REGULATION:	
‣ Credit institutions	‣ Managers of alternative investment funds
‣ Payment institutions	‣ Data reporting service providers
‣ Account information service providers	‣ Insurance and reinsurance undertakings
‣ Electronic money institutions	‣ Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
‣ Investment firms	‣ Institutions for occupational retirement provision
‣ Crypto-asset service providers and issuers of asset-referenced tokens	‣ Credit rating agencies
‣ Central securities depositories	‣ Administrators of critical benchmarks
‣ Central counterparties	‣ Crowdfunding service providers
‣ Trading venues	‣ Securitisation repositories
‣ Trade repositories	‣ ICT third party service providers
‣ Management companies	

Why DORA?

DORA "acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories."[3] The DORA regulatory framework lays out requirements that address the security of financial entities' networks and information systems to enhance cybersecurity across the EU's financial sector. This helps financial entities reduce the potential impact of digital threats on their business continuity, legal liability, and financial and reputational loss.

Requirements of DORA

In order to achieve a high common level of digital operational resilience, this Regulation lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities[4] as follows:

1. **ICT Risk Management**: Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience.[5]
2. **ICT-Related Incident Management Process**: Financial entities shall record all ICT-related incidents and significant cyber threats. Financial entities shall establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.[6]
3. **Digital Operational Resilience Testing**: To ensure that financial entities are prepared to tackle ICT-related incidents, DORA defines common standards with a focus on resilience testing by these entities, "such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing."[7]

4. **ICT Third-Party Risk Management (TPRM)**: Recognizing the increasing importance of third-party ICT service providers, DORA requires financial entities to "manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework"[8] through contractual agreements like accessibility, availability, integrity, security, and protection of personal data; clear termination rights; and more.

5. **Information and Intelligence Sharing**: With the aim of boosting the collective ability of financial institutions to identify and combat ICT risks, DORA encourages them to "exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:

   A. aims to enhance the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages;

   B. takes place within trusted communities of financial entities;

   C. is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data in accordance with Regulation (EU) 2016/679 and guidelines on competition policy."[9]

6. **Oversight Framework of Critical ICT Third-Party Providers**: The Joint Committee, in accordance with Article 57(1) of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, shall establish the Oversight Forum as a sub-committee for the purposes of supporting the work of the Joint Committee and of the Lead Overseer referred to in Article 31(1), point (b), in the area of ICT third-party risk across financial sectors. The Oversight Forum shall prepare the draft joint positions and the draft common acts of the Joint Committee in that area.

The Oversight Forum shall regularly discuss relevant developments on ICT risk and vulnerabilities and promote a consistent approach in the monitoring of ICT third-party risk at Union level.[10]

DORA and NIS 2

DORA and NIS 2 are two critical pieces of EU cybersecurity legislation. The NIS 2 Directive (Directive (EU) 2022/2555) is a legislative act that aims to achieve a high common level of cybersecurity across the European Union.[11]

The relationship between DORA and NIS 2 is that NIS 2 aims to improve cybersecurity and protect critical infrastructure in the EU, whereas DORA addresses the EU financial sector's increasing reliance on digital technologies and aims to ensure that the financial system remains functional even in the event of a cyberattack.

What is significant to note is that NIS 2 is a European directive. By 17 October 2024, Member States must adopt and publish the measures necessary to comply with the NIS 2 Directive[11]. DORA is a European regulation[12] that will be applicable as it stands in all EU countries from January 17, 2025.

Article 1(2) of DORA provides that, in relation to financial entities covered by the NIS 2 Directive and its corresponding national transposition rules, DORA shall be considered a sector-specific Union legal act for the purposes of Article 4 of the NIS 2 Directive.[12] DORA is "lex specialis" to NIS 2[13,14] for the financial sector, a principle that states that a specific law takes precedence over a general one. So, for financial entities covered under DORA, this text prevails over NIS2. However, this does not mean that NIS 2 obligations are no longer applicable to entities affected by both texts.

Penalties for DORA Non-Compliance

The potential penalties associated with DORA can be significant and, differently to GDPR and/or NIS(2), encourage the firm to comply by imposing fines on a daily basis. Those organisations deemed noncompliant by the relevant supervisory body may find themselves subject to a periodic penalty payment of 1% of the average daily global turnover in the preceding year, for up to six months, until compliance is achieved. The supervisory body may also issue cease-and-desist orders, termination notices, additional pecuniary measures, and public notices[15].

DORA Timelines

DORA was first proposed by the European Commission in September 2020. It came into force on 16 January 2023. Financial entities and third-party ICT service providers have until January 17, 2025, to prepare for DORA and implement it. Batch 1 of the Regulatory Technical Standards, or RTS, and the Implementing Technical Standards (ITS) were published on 17 January 2024. Batch 2 of these standards is under consultation.

1. The emphasis on "financial entities" rather than "financial institutions" demonstrates the EU's approach to addressing the digital operational resilience of the financial sector in a holistic manner, recognizing the interconnected and digital nature of today's financial systems. This approach ensures that the regulatory framework can adapt to the evolving landscape of financial services, where traditional boundaries between different types of financial activities have become increasingly blurred.
2. Conversely, Section 2, paragraph 3 also identifies entities to which DORA does not apply, including managers of alternative investment funds, insurance and reinsurance undertakings, institution for occupational retirement that operate pension schemes, legal persons exempted by other EU Acts, insurance and reinsurance and ancillary insurance intermediaries, and post office giro institutions.
3. https://www.digital-operational-resilience-act.com/#:~:text=DORA%20sets%20uniform%20requirements%20for,platforms%20or%20data%20analytics%20services.
4. https://www.digital-operational-resilience-act.com/Article_1.html
5. https://www.digital-operational-resilience-act.com/Article_6.html
6. https://www.digital-operational-resilience-act.com/Article_17.html
7. https://www.digital-operational-resilience-act.com/Article_25.html
8. https://www.digital-operational-resilience-act.com/Article_28.html
9. https://www.digital-operational-resilience-act.com/Article_45.html
10. https://www.digital-operational-resilience-act.com/Article_32.html
11. https://www.nis-2-directive.com/
12. https://www.digital-operational-resilience-act.com/
13. https://www.dora-info.eu/dora/recital-16/
14. https://www.ebf.eu/wp-content/uploads/2021/06/EBF-key-messages-on-NIS2-proposal.pdf
15. https://www.orrick.com/en/Insights/2023/01/5-Things-You-Need-to-Know-About-DORA

2024-04-09 (WP-MP)

SOPHOS