ERMIS

Newsletter

March 2025 - Issue No 3

In this Issue

The DORA Regulation: Enhancing Digital Operational Resilience in the Financial Sector

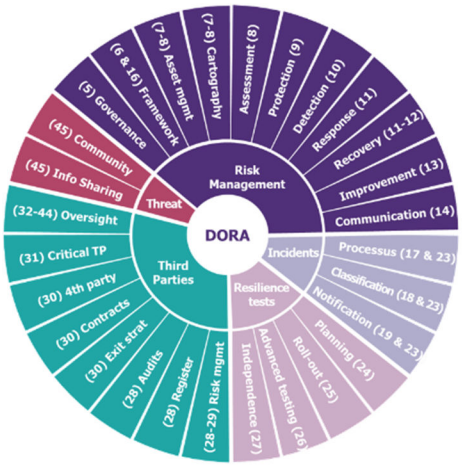
The recently enacted Regulation 2022/2554, also known as the Digital Operational Resilience Act (DORA), aims to bolster the digital operational resilience of financial institutions across the European Union, ensuring they can withstand, respond to and recover from ICT-related disruptions and threats.
DORA entered into force on January 16, 2023. Throughout 2024, financial institutions and ICT third-party service providers asked to prepare and implement the required frameworks and processes. Full compliance with DORA is mandatory by mid-January 2025.

Aim: The primary goal of DORA is to enhance digital resilience by establishing robust frameworks to manage ICT risks and ensure the continuity of financial services. It aims to harmonize ICT risk management by creating uniform requirements across the EU for managing ICT risks in the financial sector. Additionally, DORA seeks to strengthen incident response by improving the detection, management, and reporting of ICT-related incidents.

Requirements: Financial institutions are required to establish comprehensive ICT risk management frameworks. These frameworks should include governance, protection, detection, response, and recovery measures. Institutions must detect, manage, and report ICT-related incidents, with major incidents being reported to competent authorities to ensure timely and effective responses.

Institutions must manage risks associated with ICT third-party service providers. Contracts with third-party providers must include specific provisions for security, data protection and termination rights. An oversight framework is established for critical ICT third-party service providers, with the designation of critical providers and the role of the Lead Overseer to ensure compliance. Furthermore, financial institutions are encouraged to share cyber threat information and intelligence within trusted communities.

Competent authorities, such as the European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority will regularly monitor financial institutions and ICT third-party service providers to ensure compliance with DORA. This includes conducting on-site and off-site inspections. Authorities have the power to impose administrative penalties for breaches of DORA including fines, orders to cease non-compliant conduct and public notices. They can also require financial institutions to take corrective actions to address non-compliance. Collaboration between national and EU bodies, such as the ESAs and the ECB will ensure consistent enforcement.



Impact: The coexistence of NIS2 and DORA is described in both regulations. NIS2 (Directive on Security of Network and Information Systems) aims at enhancing the security of network and information systems across the European Union. It provides a broad cybersecurity framework for essential and important sectors while DORA ensures financial institutions meet stricter, sector-specific operational resilience standards.
DORA marks a significant step towards enhancing the digital operational resilience of the financial sector in the EU. By establishing robust frameworks for managing ICT risks and ensuring compliance, DORA aims to create a more secure and resilient financial environment.

By Vasilis Kakariaris,
Karavias Underwriting Agency

2nd Plenary Meeting

The Consortium held its 2nd plenary meeting in Athens, Greece on February 17th and 18th, 2025. All partners gathered to assess progress and synchronize key project objectives. Discussions focused on the advancement of the Work Packages and strategizing the upcoming steps in view of the upcoming midterm review.

Cyber Insurance Workshop

We are pleased to announce the successful completion of our workshop, held on February 18th, 2025. Participants had the opportunity to learn about the latest developments in cyber insurance, as well as to exchange views and experiences with insurance providers.

Cyber Insurance – A Client SME's Perspective

In an era where cyber threats continue to escalate, Small and Medium-sized Enterprises (SMEs) are increasingly recognizing the importance of Cyber insurance as a tool for risk mitigation. However, navigating the regulatory landscape can be challenging, as European Union regulations shape both the requirements and expectations around cybersecurity and insurance coverage. Several regulations came into force and may ease SMEs seeking Cyber insurance.

The **General Data Protection Regulation (GDPR)** was the first measure towards this direction, affecting SMEs in the EU. Companies that handle personal data must ensure compliance with stringent security and reporting requirements. A data breach can result in severe financial penalties (up to €20 million or 4% of global turnover), making cyber insurance an attractive safeguard. Many insurers assess an SME's GDPR compliance when determining coverage and premiums, reinforcing the need for robust cybersecurity measures.

The **Network and Information Security Directive 2 (NIS2)**, already in effect since October 2024, expands cybersecurity obligations beyond large organizations to include key SMEs in critical sectors such as healthcare, finance, and digital infrastructure. SMEs falling within its scope must implement risk management practices, conduct regular security assessments, and ensure incident reporting. Non-compliance may lead to financial penalties (Critical entities: up to €10 million or 2% of total worldwide annual turnover, Important organizations: up to €7 million or 1.4% of worldwide annual turnover)* and reputational damage—factors that insurers consider when underwriting cyber policies.

The **Artificial Intelligence Act (AI Act)**, expected to be enforced in 2025, while not a cybersecurity-specific regulation, affects SMEs developing or using AI systems, particularly in high-risk sectors such as finance, healthcare, and critical infrastructure. It introduces requirements for transparency, risk assessments, and data governance. SMEs relying on AI-driven cybersecurity solutions or handling sensitive AI-generated data must ensure compliance. Cyber insurance policies may increasingly consider AI-related risks, including algorithmic failures or biases, as part of their coverage scope.

Finally, the **Cyber Resilience Act (CRA)**, expected to be fully adopted in 2025, introduces security-by-design requirements for digital products and services. SMEs developing or using software and connected devices must ensure compliance to mitigate liability risks. Cyber insurance policies may evolve to reflect these new regulatory obligations.

What SMEs Should Consider Before Obtaining Cyber insurance

For SMEs, securing cyber insurance is not just about transferring risk—it's also about demonstrating resilience. Insurers increasingly demand evidence of risk management practices, including data encryption, employee training, and incident response plans. Thus, aligning with EU regulations can help SMEs obtain better insurance premiums and ensure that policies cover regulatory fines and legal costs. As EU regulations evolve, SMEs must stay informed and proactively strengthen their cybersecurity posture. Cyber insurance, when aligned with compliance efforts, can serve as a vital safety net against ever-growing cyber risks.

** NIS2 Art. 34 Par 4, 5*

By George Alexandris,
Nodalpoint Systems

Contact

Project Coordinator Zelus **Inquiries** info@dep-ermis.eu

Disclaimer

The project received funding under Grant Agreement No 101128013, and is supported by the European Cybersecurity Competence Centre.

The project is supported by the Ministry of Digital Governance of Hellenic Republic and the National Cyber Security Authority and is aligned with the Hellenic Cyber Security Strategy.

Consortium Partners