Financial Services Briefing: Special Edition

Digital Operational Resilience Act (DORA): Where do we stand?

A. **Consolidation of the Regulatory Framework and Activation of Oversight Mechanisms**
B. **Oversight of Critical ICT Third-Party Providers**
C. **Incident Reporting and Data Quality**
D. **Resilience Testing and TLPT**
E. **Developments in Greece**
F. **Outlook for 2026 and Beyond**

Following a two-year implementation period after entering into force, the Digital Operational Resilience Act (Regulation (EU) 2022/2554 – **DORA**) became fully applicable in January 2025, setting a harmonized, directly applicable regulatory framework for digital operational resilience in the EU financial sector. A little over a year later, the focus is shifting from the definition of the regulatory framework to its implementation in practice. Supervisory expectations have become more concrete; the technical standards are now largely in place and National authorities are shaping the framework's operation in practice. This briefing provides an overview of the EU level developments and their implementation in Greece.

A. Consolidation of the Regulatory Framework and Activation of Oversight Mechanisms

1. Over the past year, the European Supervisory Authorities (**ESAs**[1]) have finalised the Regulatory and Implementing Technical Standards (**RTS/ITS**) to further specify certain DORA requirements. These standards provide detailed and prescriptive guidance on issues including ICT risk

[1] The European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority.

management, classification of ICT-related incidents and cyber threats, incident reporting and notification, governance arrangements, resilience testing.

2. At the same time, the regulatory framework is evolving into an active, operational supervisory mechanism. This shift is reflected in a number of ways including in the:
   a. designation of critical ICT third-party providers;
   b. introduction of a direct ESA-led oversight framework;
   c. deployment of Joint Examination Teams; and
   d. increased emphasis on structured data reporting and incident reporting, including governance and data quality, as detailed in the ESA Guide on DORA Oversight Activities (July 2025).

B. Oversight of Critical ICT Third-Party Providers

1. DORA introduces an EU level oversight regime for critical ICT third party providers (**CTPPs**). The ESAs, acting as Lead Overseers, are empowered to conduct inspections, request information and issue recommendations directly to ICT providers deemed critical to the financial system.
2. This development is already reshaping contractual dynamics between financial entities and ICT providers, particularly in areas such as audit and access rights, data portability, subcontracting arrangements and exit strategies. In practice, contract remediation and renegotiation processes have been driven by the obligation to submit ICT third-party registers, which required firms to map their ICT dependencies and address gaps in existing contractual arrangements.

C. Incident Reporting and Data Quality

1. Incident reporting emerged in 2025 as a central operational pillar of DORA implementation. The application of the relevant RTS/ITS has introduced highly granular and standardised requirements in relation to the classification of ICT-related incidents and cyber threats, reporting timelines and data templates.
2. In practice, the relevant RTS/ITS applied in 2025 have placed particular emphasis on data quality, consistency and completeness. Supervisory expectations have focused on the ability of firms to accurately classify incidents, produce structured and timely reports and ensure robust governance over reporting processes, including clear allocation of responsibilities, defined escalation procedures and effective internal controls.

D. Resilience Testing and TLPT

1. Digital operational resilience testing has also moved to the forefront of DORA implementation in 2025, with increasing supervisory attention on firms' practical readiness to withstand and respond to ICT disruptions. In particular, the framework for advanced testing, including threat-led penetration testing (TLPT), is progressively being implemented, requiring capabilities that go

beyond standard testing and reflect realistic threat scenarios.

E. Developments in Greece

1. Law 5193/2025[2] (the **Law**) transposed the so-called DORA Directive[3] into Greek Law and aligned existing Greek financial sector legislation with its requirements. The Law allocated supervisory responsibilities between the Bank of Greece, which oversees credit institutions, payment and electronic money institutions, insurance firms and other entities within its remit, and the Hellenic Capital Market Commission, which supervises investment firms, fund managers and capital markets participants. Both authorities are vested with broad supervisory powers, including the ability to conduct on-site inspections, request information and impose administrative sanctions.
2. Greek institutions are generally progressing in their implementation efforts, although in many cases full compliance with DORA remains a key challenge, particularly following the 2025 application of the RTS/ITS and related operational requirements.

F. Outlook for 2026 and Beyond

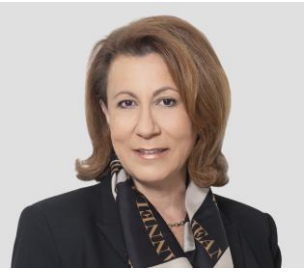
1. Looking ahead, the focus is expected to shift from implementation to supervisory convergence and enforcement. In particular, the ESA oversight framework, including the supervision of critical ICT third-party providers, is likely to intensify, supported by risk-based supervisory tools and cross-border coordination.
2. Supervisory attention is expected to remain focused on effective ICT-related risk management as well as incident reporting, data quality and resilience testing as key indicators of operational resilience. Further convergence is also anticipated through ESA-level outputs (such as Q&As and guidelines), contributing to a more consistent application of DORA across Member States.

[2] Articles 153 et s.

[3] Directive (EU) 2022/2556.

KEY CONTACTS

Maria Nefeli Bernitsa
Partner
mnbernitsa@bernitsaslaw.com



Dr. Anastasia Mallerou
Counsel
amallerou@bernitsaslaw.com

This Briefing is intended to provide general information and is not meant to constitute a comprehensive analysis of the matters set out herein or to be relied upon as legal advice. It is not meant to create a lawyer-client relationship. Legal and other professional advice should be sought before applying any of the information in this Briefing to a specific situation.
Bernitsas Law Firm is a partnership of attorneys regulated by Presidential Decree 81/2005 and Law 4194/2013, as currently in force, with its registered address at 5 Lykavittou Street, Athens 106 72, Greece. If you no longer wish to receive Briefings from us, please click here to Unsubscribe.