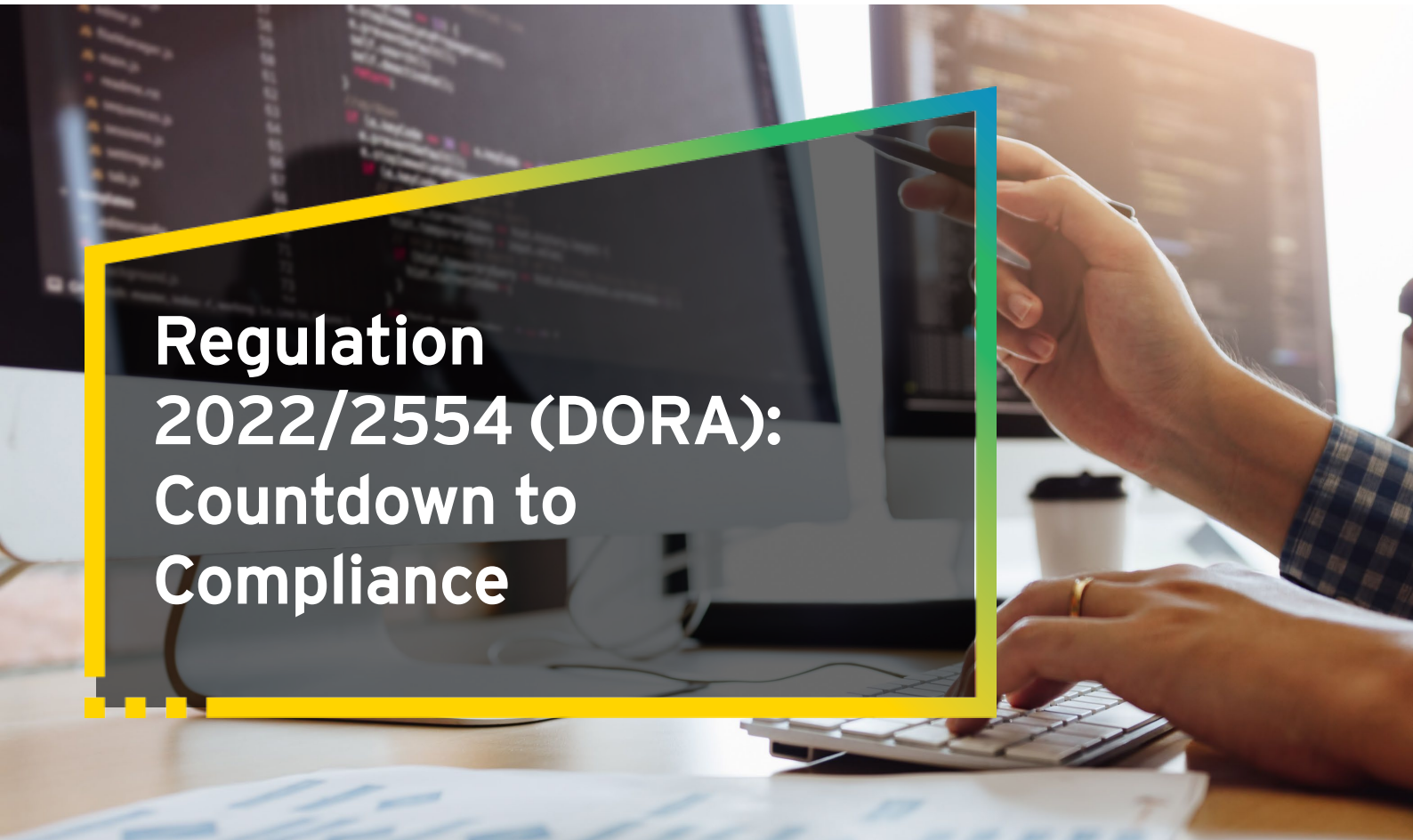


**Platis - Anastassiadis  
& Associates**

The associate law firm of EY Greece



# Regulation 2022/2554 (DORA): Countdown to Compliance

Regulation 2022/2554 “Digital Operational Resilience Act” (DORA) is a landmark regulatory framework designed to enhance the digital resilience of financial institutions across the European Union. It sets forth mandatory requirements for managing ICT risks and ensuring business continuity in the face of cyber threats, operational disruptions, and third-party vulnerabilities.

**The key objectives of DORA include:**

- **ICT Risk Management:** Establish and maintain robust frameworks to identify, monitor, and manage ICT-related risks.
- **Operational Resilience Testing:** Implement advanced testing strategies, including penetration testing, to ensure systems remain functional under stress.
- **Incident Reporting:** Mandate timely and structured reporting of ICT-related incidents to relevant regulatory authorities.
- **Third-Party Risk Management:** Ensure ICT service providers adhere to DORA requirements by including specific provisions in contracts.
- **Resilience of the Financial Sector:** Align industry-wide practices for a unified response to digital and operational threats.

**Countdown to Compliance - The Clock is Ticking**

The DORA has entered into force on 16 January 2023 and will apply as of 17 January 2025.

Financial institutions must act swiftly to implement DORA's provisions. Waiting until the last-minute risks non-compliance and significant operational challenges.

**1. Scope**

The services in scope include ICT services, which encompass a broad range of offerings, extending beyond traditional outsourced IT services.

The entities in scope include:

- Financial institutions (i.e. credit institutions, payment institutions, insurance and reinsurance undertakings)
- ICT third-party service providers

## 2. The 'five pillars' of DORA

### Pillar 1: ICT Risk Management

- Governance and organization
- ICT risk management framework
- Management of ICT systems, protocols and tools
- Identification and classification of ICT systems
- Protection, prevention and detection of ICT systems
- ICT business continuity, response and recovery and communication plans
- Back-up policies, restoration and recovery procedures
- Post incident reviews and lessons learned

### Pillar 2: ICT-incident classification and reporting

- ICT-related incident management process
- Classification of ICT-related incidents and cyber threats
- Reporting of major ICT-related incidents & voluntary notification of significant cyber threats

### Pillar 3: Digital operational resilience testing

- Digital operational resilience testing programme
- Testing of ICT tools and systems
- Advanced testing of ICT tools, systems, and processes based on TLPT
- Requirements for TLPT testers

### Pillar 4: ICT third-party risk management

- ICT third-party risk management strategy and procedures
- Register of information
- Contractual arrangements
- Right to audit
- Exit strategies and plans
- ICT concentration risk & subcontracting risks

### Pillar 5: Information-sharing arrangements

- Newly introduced for financial entities
- (Voluntary) information sharing arrangements on cyber threat information and intelligence

## 3. DORA Supervisory Framework for the financial sector

### Powers granted to the NCAs:

NCAs shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under DORA, including at least:

- Access to any document or data held in any form that the NCA considers relevant for the performance of its duties and receive or take a copy of it
- Carry out on-site inspections or investigations
- Require corrective and remedial measures for breaches of the requirements of DORA

### Penalties NCAs can impose:

- Administrative penalties
- Remedial measures
- Criminal penalties (if the breach in question is subject to criminal penalties under the national law of the MSs)

### Factors considered when determining penalties:

- Extent to which the breach is intentional or results from negligence
- Materiality, gravity and duration of the breach
- Responsibility
- Level of cooperation
- Losses for third parties
- Financial strength of the person responsible
- Importance of profits gained or losses avoided

### Functions of NCAs:

- Oversight on critical ICT TPPs
- Cooperation and assistance to the Lead Overseer with regard to the Oversight Framework
- Follow-up of Lead Overseer recommendations
- ICT-related incidents
- Receive major ICT-related incident reports
- Provide relevant and proportionate supervisory feedback
- Threat-led penetration testing (TLPT)
- Validate TLPT scope
- Provide attestation confirming TLPT according to requirements
- Identify FEs required to perform TLPT
- Approve the use of internal testers
- Reviewing Contractual arrangements on the use of ICT TPPs by Fes Including annual reports, register of information upon request and CIFs

## 4. Implementation of DORA within your organization

Under the provisions of the DORA, this management body (those who effectively run the entity or hold key functions in accordance with relevant Union or national law) of the financial institution is responsible and liable for the proper implementation of legal requirements.

Competent authorities thus have the explicit power to apply administrative penalties (e.g., fines) to members of this management body. Therefore, it is crucial for the management body to be actively involved in the implementation and monitoring of DORA requirements.

Certain new and binding DORA requirements are highly specific in nature, necessitating a thorough analysis of maturity to achieve effective implementation. This includes, but is not limited to, third-party contracts and potential re-negotiations.

Requirements that are not fully specified in DORA are further elaborated upon in the Regulatory Technical Standards (RTS) of the ESAs. Although the RTS do not introduce new obligations, they provide specifications that require implementation.

The Greek supplementary Act to DORA, which will among others designate the supervisory authorities for its oversight, is still pending.

The DORA Regulation 2022/2554 is available [here](#).

## About Platis - Anastassiadis & Associates

Platis - Anastassiadis & Associates is part of the EY Law network operating in 90 countries globally and is comprised of 3,500+ people.

We are an independent law office with a core team of 45 lawyers. Our office provides high quality legal services across the full range of commercial and financial transactions.

Especially in our geographical area, we have established an ongoing cooperation with the respective law firms which are associated with EY, in order to offer seamless and consistent regional services to our clients that have cross country operations.

Our experience allows us to better understand our clients' needs and offer them integrated multidisciplinary solutions in the fields of accounting, tax and financial advisory services. Platis - Anastassiadis & Associates law office is solution focused. We work closely with our clients to seek innovative and practical ways of dealing with their issues. Our priority is to help our clients meet their business objectives. Our expertise, commitment and enthusiasm has resulted in the build up of a client base which includes local and international listed, state and private sector companies and financial institutions.

For more information on digital law issues, please contact:

### **Eirinikos Platis**

Partner

[eirinikos.platis@gr.ey.com](mailto:eirinikos.platis@gr.ey.com)

### **Antonios Broumas**

Senior Manager

[antonios.broumas@gr.ey.com](mailto:antonios.broumas@gr.ey.com)

at the

### **Platis - Anastassiadis & Associates Law Partnership**

Tel.: +30 210 2886 512

[legaloffice@gr.ey.com](mailto:legaloffice@gr.ey.com)

© 2025

All rights reserved

[ey.com](http://ey.com)



EY



EY Greece



eygreece



@EY\_Greece



EY Greece

Platis - Anastassiadis & Associates Law Partnership is associated with EY.

Partners: E. Platis, A. Anastassiadis

Partnership is registered with the Athens Bar, registration number 80240

List of our associates upon request.

This document contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global EY organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.