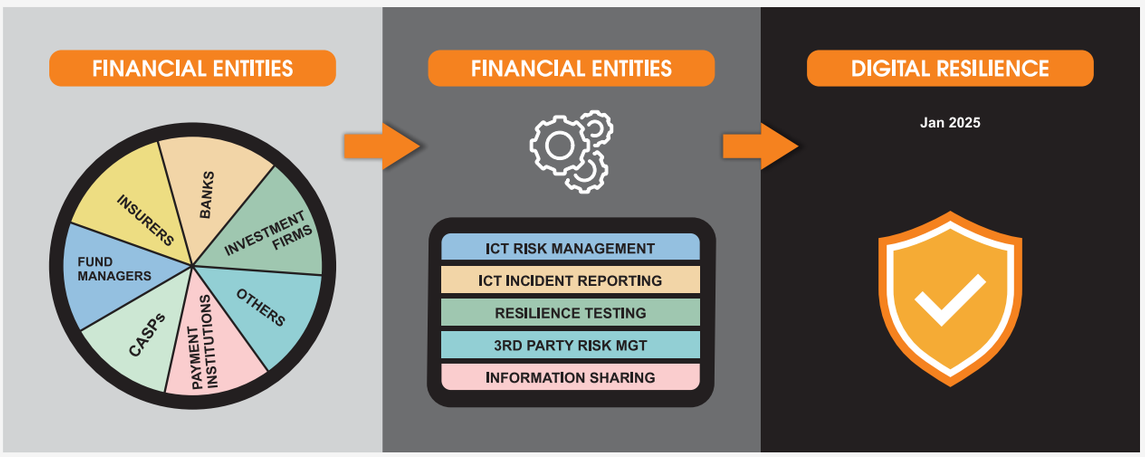
DIGITAL OPERATIONAL RESILIENCE ACT

ELIAS NEOCLEOUS & Co LLC

EU Regulation 2022/2554 on Digital Operational Resilience ("DORA"), fully applicable from 17 January 2025 is designed to establish a consolidated and harmonized framework at EU level for ensuring the digital resilience and ICT security of financial entities. DORA sets the bar particularly high by introducing a long and detailed list of complex requirements, supplemented by several delegated and implementing acts.
By January 2025, large and small financial entities such as banks, insurers, investment firms, and fund managers, will need to have in place intrinsic arrangements for comprehensive ICT risk management (strategies, policies, technical systems, protocols, tools), resilience testing and incident reporting processes, mechanisms for managing ICT third party risks, and information sharing arrangements. National competent authorities are granted the power to impose sanctions, including fines, on non-compliant entities once the rules apply in 2025.



On 17 January 2024 the European Supervisory Authorities (ESAs) submitted for adoption to the Commission the first set of draft regulatory and implementing technical standards under DORA (3 RTS and 1 ITS). A second batch is expected in July 2024 (4 RTS, 1 ITS, and guidelines).

IN-SCOPE ENTITIES

On 17 January 2024 the European Supervisory Authorities (ESAs) submitted for adoption to the Commission the first set of draft regulatory and implementing technical standards under DORA (3 RTS and 1 ITS). A second batch is expected in July 2024 (4 RTS, 1 ITS, and guidelines).

LIGHTER DORA REQUIREMENTS

- Microenterprises (less than 10 staff, Turnover and/or B/S up to €2 million)
- Small and non-interconnected investment firms
- Small occupational pension schemes
- Entities exempted under the Capital Requirements Directive or the Payment Services Directive or the E-Money Directive

In addition to financial entities, the Regulation also applies to ICT 3rd party services providers that are designated as critical for financial entities ("critical ICT 3rd party service providers"). Moreover, DORA constitutes lex specialis with regard to the Network and Information Security Directive 2022/2555/EU ("NIS 2") that sets out horizontal cybersecurity requirements for critical sectors and essential services.

FIVE PILLARS IN THE REGULATION

DORA requires financial entities to have in place an internal governance and control framework that ensures effective ICT risk management and cyber-threat resilience. The board is ultimately responsible for managing the entity's ICT risks and is expected to put in place elaborate policies, procedures, systems and other arrangements to ensure strong and effective compliance with the Regulation's various requirements under the five pillars below:

In line with the principle of proportionality, the most complex and demanding governance and technical requirements of DORA do not apply to very small or low-risk entities such as microenterprises and small and non-interconnected investment firms. Where a provision of the Regulation is not applicable to such entities (i.e having a strategy on 3rd party ICT risk), specific wording to that effect is included in the text of the relevant provision. It is notable that while the Regulation exempts certain entities such as small and non-interconnected investment firms from the provisions relating to the ICT risk management framework (pillar 1), it concurrently obliges them to have in place an alternative (simplified) risk management framework that is quite demanding and accompanied by detailed rules set out in delegated acts.

The requirements with respect to the management of 3rd party ICT risk can be quite challenging. Entities should meticulously review contractual arrangements, and ensure that these include audit, access and inspection rights, appropriate termination, transition and exit rights, recovery and return of data, and several other performance and security provisions. Where ICT services support critical functions, additional obligations apply with respect to contract contents.

Broad definition of "ICT Services" under DORA: "digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis", including electronic communication services but excluding traditional analogue telephone services.

CONSIDERATIONS AND CHALLENGES FOR FINANCIAL ENTITIES

DORA requires financial entities to have in place an internal governance and control framework that ensures effective ICT risk management and cyber-threat resilience. The board is ultimately responsible for managing the entity's ICT risks and is expected to put in place elaborate policies, procedures, systems and other arrangements to ensure strong and effective compliance with the Regulation's various requirements under the five pillars below:

DETERMINE WHETHER AND HOW DORA AFFECTS YOUR FIRM

As a first step, a financial entity should determine whether it falls within the scope of DORA. An in-scope entity should also determine whether it qualifies as a financial entity for which lighter requirements or exemptions apply and identify all the relevant provisions and requirements. Investment firms in particular should examine the technical criteria set out in the EU's Investment Firms Regulation for qualifying as a "small and non-interconnected investment firm".

CARRY OUT A GAP ANALYSIS

Obtain an in-depth understanding of the structures and capabilities that need to be put in place, and assess the gap compared to the existing ICT risk management infrastructure. An inventory and review of existing contractual arrangements with 3rd party ICT services providers is recommended, to determine the gap with respect to provisions on performance, access, termination, exit and other rights.

DESIGN, BUILD AND IMPLEMENT POLICIES AND PROCEDURES

Compliance with DORA's requirements under each of the five pillars, such as continuous identification of ICT risk sources, system monitoring and anomaly detection, security of ICT systems, business continuity and recovery planning, backup and restoration, recording and reporting incidents, regular testing, reviewing 3rd party ICT contractual arrangements and formulating DORA-compliant contracts, necessitates the creation of several elaborate policies, procedures, and mechanisms that together form a coherent and effective company-wide cybersecurity framework.

This can be a daunting project for many companies given the extent and complexity of the technical and organizational changes needed, the need for effective cross-functional coordination, specific expertise, and the considerable resources required. Use of external consultants with know-how in designing and implementing a DORA-compliant ICT infrastructure should be seriously considered, especially in the case of financial entities that do not possess in-depth internal expertise in ICT risk management.

WE ARE HERE TO HELP

We possess industry-leading experience in assisting financial entities to interpret and implement complex regulatory frameworks, set up appropriate structures, policies and systems, and ensure full and effective regulatory compliance. Our multidisciplinary team of lawyers, financial services specialists, compliance experts, and ICT and cybersecurity professionals is here to help you devise and implement a best-suited Dora-compliant ICT framework.

Connect with our Tech Law team to discuss DORA and explore how we can support you.