DORA: A step towards enhanced cybersecurity and digital resilience in the financial services sector.

By Adonis Zachariou and Theodora Alexandrou, Associates, Elias Neocleous & Co LLC.

As part of the new strategy on digital finance for the European Union ("EU") financial sector, on 10 November 2022 the European Parliament approved the Digital Operational Resilience Act ("DORA").
The act is a legislative piece reflecting the EU's efforts towards creating a consistent incident reporting mechanism. Its objectives are to reduce administrative burdens for financial entities and strengthen supervisory effectiveness across the EU.

WHAT IS DORA

DORA aims at establishing a clear set of rules for 'in-scope' financial entities ("ISFEs") and their Information and Communications Technology ("ICT") providers so as to unify IT risk management, define a procedure for in-depth testing of IT systems, and increase the awareness of supervisory authorities regarding cyber risks. In essence, this will provide a more clear-cut digital risk assessment across the EU financial sector. Consequently, this will ensure that the necessary measures are put in place to protect the EU against cyberattacks and other cyber-fraud related incidents.

IN-SCOPE FINANCIAL ENTITIES (ISFES)

In order to ensure consistency around the ICT risk management requirements applicable to the financial sector, DORA covers a (non-exhaustive) broad range of financial entities regulated at EU level, such as:

- Credit, payment and electronic money institutions;
- Investment firms;
- Crypto-asset service providers (as authorized under the Markets in Crypto-Assets 'MiCA' regulation);
- Central securities depositories and counterparties;
- Trading venues, trade repositories;
- Managers of alternative investment funds (AIFs) and management companies;
- Data reporting service providers, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;
- Institutions for occupational retirement pensions;
- Credit rating agencies;
- Statutory auditors and audit firms;
- Administrators of critical benchmarks; and
- Crowdfunding service providers.

OUT-OF-SCOPE FINANCIAL ENTITIES

The Commission will continue to assess the necessity of a further extension of DORA's scope and any impacts associated with this. Currently DORA does not provide for certain categories of entities and ICT infrastructure such as (i) system operators (as defined in point (p) of Article 2 of Directive 98/26/EC22) on settlement finality in payment and securities settlement systems ("SFDs"), or (ii) any system participant not being itself a financial entity regulated at EU level (i.e., credit institution, investment firm, central counterparties ("CCPs")). The EU registry for emission allowances operating in accordance with Directive 2003/87/EC under the aegis of the European Commission also falls outside of DORA's scope.

OBLIGATIONS ON ISFES UNDER DORA

DORA introduces 6 main measures that ISFEs and their ICT providers should adopt. The measures are as follows:

1. Governance related requirements – the risk management bodies should have an active role in steering the ISFE's ICT risk management framework through:

- **The allocation of clear roles and responsibilities for all ICT-related functions;**
- **Full-on monitoring of the ICT risk management; and**
- **Approval and control processes together with the allocation of ICT investments and trainings.**

2. ICT risk management requirements – ISFEs will need to set-up and maintain resilient ICT systems and tools which should identify, respond to, and minimize the impact of ICT risks on a continuous basis. Concurrently they should put in place business continuity policies, and disaster and recovery plans, in order to respond and cope with possible breaches in time.

3. ICT-related incident reporting – ISFEs are required to establish and implement a management process to monitor and record ICT-related incidents (using a common template), while classifying them depending on their impact and severity. Such incidents should be reported to the competent authorities through a harmonized procedure developed by the European Supervisory Authorities ("ESAs").

4. Digital operational resilience testing – the measures and precautions put in place by the ISFEs should be regularly tested and updated for preparedness and identification of weaknesses and deficiencies. ISFEs identified as 'significant and cyber mature' by the ESAs will also be required to conduct advanced testing based on threat led penetration tests as a controlled attempt to compromise the cyber resilience of the ISFE by simulating the tactics, techniques, and procedures of real-life threat actors.

5. ICT third-party risk – contracts which govern the relationship of ISFEs' monitoring of risk arising through ICT third-party providers should be extremely thorough and provide for all stages of their pre, intra and post-contractual relationship. Furthermore, ICT third-party service providers which may be classified as 'critical' by ESAs should be subjected to an EU oversight framework. This is to ensure that technology services providers fulfilling a critical role to the functioning of the financial sector are adequately monitored on a Pan-European scale.

6. Information sharing - ISFEs can set-up arrangements to exchange, amongst themselves, cyber threat information and intelligence. This is designed to minimize the spread of the threat and support ISFEs' monitoring of risk arising through ICT third-party providers' defensive capabilities and threat detection techniques.

These measures will apply proportionately depending on the size and business profile of each ISFE and its exposure to digital risk. For instance, it will not be mandatory for ISFEs qualifying as microenterprises to regularly conduct risk analyses on the legacy of the ICT systems, perform in depth assessments after major changes in the network and information system infrastructure, establish governance arrangements etc. However, such measures should be reasonably taken by larger ISFEs having more resources. In addition, penetration tests will be obligatory only for ISFEs identifying as significant for the purpose of advanced digital resilience testing.

CLOSING REMARKS

DORA is a methodical attempt towards creating a robust cyber-security model, the standards of which all ISFEs will be required to comply with. The latest proposal on the amendment of the existing Network and Information Security Directive (NIS) was also approved by the EU Parliament on the 10th of November ("NIS2"). NIS2 extends cybersecurity and cyber risk management requirements to other 'essential' and 'important' entities outside the financial services sector. NIS2 and DORA together aim to form a harmonized EU-wide cyber-security and risk assessment system between the Member States.

Although DORA still requires the approval of the European Council to enter into force as a regulation, it would be prudent for ISFEs to take measures and start preparing their organizations for these important requirements and changes. Some of the requirements will require significant resource allocation and specific arrangements to be made within the organizations. Failure to prepare early may result in some ISFEs struggling to comply in time.

DORA will apply 24 months after the date it enters into force as a regulation and shall be binding in its entirety in all the Member States.

HOW CAN WE HELP YOU?

Our specialists and dedicated services can help you design and implement your business strategy in compliance with DORA.

For more information on the above please speak with our Tech Law team or your usual contact at Elias Neocleous & Co LLC.

Authors: Adonis Zachariou,
Theodora Alexandrou,
Associates, Elias Neocleous & Co LLC.