ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

Key aspects of the implementation of DORA

The Cyprus Securities and Exchange Commission ('CySEC') wishes to outline the key aspects for the implementation of the new framework on Digital Operational Resilience for the financial sector.

A. Relevant Legislation

1. The framework comprises of:

i. REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 ("DORA regulation").

ii. DIRECTIVE (EU) 2022/2556 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector ("DORA Directive").

iii. Regulatory Technical Standards ('RTS') and Implementing Technical Standards ('ITS') issued by the European Commission ('EC') and developed by the joint committee of the European Supervisory Authorities[1] ('ESAs'). Note that further RTS and ITS will be issued in the coming months by the EC.

We urge you to search through the ESAs' websites on a continuous basis so as to be fully updated with the new developments.

[1] The ESAs are the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

B. Scope of Application

Applies to the entities as defined in Article 2 of DORA Regulation:

(a)credit institutions;

(b)payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;

(c) account information service providers;

(d) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;

(e) investment firms;

(f) crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of asset-referenced tokens;

(g) central securities depositories;

(h)central counterparties;

(i) trading venues;

(j) trade repositories;

(k) managers of alternative investment funds;

(l) management companies;

(m) data reporting service providers;

(n) insurance and reinsurance undertakings;

(o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;

(p) institutions for occupational retirement provision;

(q) credit rating agencies;

(r)administrators of critical benchmarks;

(s)crowdfunding service providers;

(t)securitisation repositories;

(u)ICT third-party service providers.

C. Rationale behind DORA

2. The Union financial sector is regulated by a Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and Information and Communication Technology (ICT) security were not yet fully or consistently harmonised, despite digital operational resilience being vital for ensuring financial stability and market integrity in the digital age, and no less important than, for example, common prudential or market conduct standards. The Single Rulebook and system of supervision should therefore be developed to also cover digital operational resilience, by strengthening the mandates of competent authorities to enable them to supervise the management of ICT risk in the financial sector in order to protect the integrity and efficiency of the internal market, and to facilitate its orderly functioning.

D. Proportionality principle (Article 4 of DORA Regulation)

3. The DORA is established based on the principle of proportionality, considering the size, overall risk profile, and the nature and complexity of the financial entities' services, activities, and operations.

Specifically, DORA provides:

i. Explicit exemptions for microenterprises[2]
ii. Simplified ICT risk management for small and non-interconnected investment firms [3]
iii. Framework's review frequency adjusted on occurrence, testing and previous findings
iv. Development and implementation of policies depending on the criticality of each function
v. Criteria and materiality thresholds designed in a way that they do not pose reporting burden to smaller financial entities.
vi. Exemptions for smaller entities from weekend reporting.
vii. Only major ICT-related incidents are reported
viii. Less frequent advanced testing by means of TLPT for smaller entities
ix. ICT systems, protocols and tools appropriate to the magnitude and impact of operations
x. Only critical ICT third-party service providers (TPPs) subject to oversight

E. Main areas of the DORA Regulation

4. ICT risk management

i. Financial entities should have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in order to achieve a high level of digital operational resilience (Article 5 of DORA Regulation).
ii. Financial entities should have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and

[2] As defined in Article 3(63) of DORA Regulation
[3] As defined in Article 3(34) of DORA Regulation

comprehensively and to ensure a high level of digital operational resilience (Article 6.1 DORA Regulation).

iii. In order to address and manage ICT risk, financial entities should use and maintain updated ICT systems, protocols, and tools (Article 7 of DORA Regulation).

iv. As part of the ICT risk management framework , financial entities should identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk (Article 8 of DORA Regulation).

v. As part of the ICT risk management framework , financial entities should put in place a comprehensive ICT business continuity policy which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity (Article 11 of DORA Regulation).

vi. Small and non-interconnected investment firms (Class 3 IF) should apply simplified ICT risk management framework (Article 16 of DORA Regulation). RTS specifying ICT risk management tools, methods, processes and policies regarding simplified ICT risk management framework was published on 13th March 2024.

5. ICT-related incidents

i. Financial entities should define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.

ii. Financial entities should record all ICT-related incidents and significant cyber threats. Financial entities should establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT- related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents (Article 17 of DORA Regulation).

iii. Financial entities should classify ICT-related incidents and should determine their impact (Article 18 of DORA Regulation). RTS specifying the criteria for the classification of the ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents was published on 13th March 2024. Major incidents will be reported to CySEC in order to be assessed for supervisory actions to prevent potential spill-over effects. Additionally, an Implementing Technical Standard, (ITS) will be published.

6. Digital operational resilience testing

i. For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities, other than microenterprises, should, establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework (Article 24 of DORA Regulation).

ii. Financial entities, other than entities referred to in Article 16(1) of DORA Regulation, and other than microenterprises, which are identified in accordance with Article 16(8) of DORA Regulation, should carry out at least every 3 years advanced testing by means of TLPT (Article 26 of DORA Regulation).

iii. According to article 2 of the Draft RTS the following entities under the supervision of CySEC are required to perform TLPT:

- Central securities depositories;
- Central counterparties;
- Trading venues with an electronic trading system

- Any other financial shall be required to perform TLPT, taking into account their impact, systemic character and ICT risk profile according to the assessment of the TLPT authority:

7. Managing ICT third-party risk

Financial entities should manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework and in accordance with the following principles:

(a) financial entities that have in place contractual arrangements for the use of ICT services to run their business operations should, at all times, remain fully responsible for compliance with, and the discharge of, all obligations under this Regulation and applicable financial services law;

(b) financial entities' management of ICT third-party risk should be implemented in light of the principle of proportionality, taking into account:

- the nature, scale, complexity and importance of ICT-related dependencies,
- the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities, at individual and at group level. (article 28)

As part of their ICT risk management framework, financial entities should maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

Financial entities should report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT third-

party service providers, the type of contractual arrangements and the ICT services and functions which are being provided.

8. **Information sharing**

   i. Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools.

   ii. Financial entities should notify competent authorities of their participation in the information-sharing arrangements (Article 45 of DORA Regulation)

9. **Oversight of critical third-party providers**

The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 32(1), should:

   i. designate the ICT third-party service providers that are critical [4] for financial entities, following an assessment that takes into account the criteria specified in paragraph 2;

   ii. appoint as Lead Overseer for each critical ICT third-party service provider the ESA that is responsible, in accordance with Regulations (EU) No 1093/2010, (EU) No 1094/2010 or (EU) No 1095/2010, for the financial entities having together the largest share of total assets out of the value of total assets of all financial entities using the services of the relevant critical ICT third-party service provider, as evidenced by the sum of the individual balance sheets of those financial entities.

[4] The designation shall be based on the criteria laid out in Article 31(2).

F. Entry into force and application

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

The ESAs (EIOPA, ESMA and EBA) developed Joint Q&A in order to support the application of DORA.

G. Delegated Acts

Published 13/03/2024

- Oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid

- Criteria for the designation of ICT third-party service providers as critical for financial entities

- Criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents

- Contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers

- ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework

Draft

- Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework

- Final Report on draft RTS on classification of major incidents and significant cyber threats

- Final report on draft RTS to specify the policy on ICT services supporting critical or important functions

- Final report on draft ITS on Register of Information