LYDIAN

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

Bastiaan Bruyndonckx

INFORMATION & COMMUNICATION TECHNOLOGY

2023

On 27 December 2022, the Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 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 (***Digital Operational Resilience Act*** or ***DORA***) was published in the Official Journal of the EU.

DORA sets uniform requirements for **the security of network and information systems** of companies and organisations operating in the **financial sector** as well as critical third parties which provide ICT-related services to them, such as cloud platforms or data analytics services. DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to, and recover from all types of ICT-related disruptions and threats. These requirements are homogenous across all EU member states. The core aim is to prevent and mitigate cyber threats.

I. INTRODUCTION

The aim of DORA is to achieve a high common level of digital operational resilience for the financial sector. It does so by laying down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities.

More in particular, DORA lays down:

a. requirements applicable to **financial entities** in relation to (i) information and communication technology (ICT) risk management; (ii) reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities; (iii) reporting of major operational or security payment-related incidents to the competent authorities by certain financial entities; (iv) digital operational resilience testing; (v) information and intelligence sharing in relation to cyber threats and vulnerabilities; and (vi) measures for the sound management of ICT third-party risk;

b. requirements in relation to the **contractual arrangements** concluded between ICT third-party service providers and financial entities;

c. rules for the establishment and conduct of an **oversight framework for critical ICT third-party service providers** when providing services to financial entities; and

d. rules on cooperation among **competent authorities**, and rules on supervision and enforcement by competent authorities, in relation to all matters covered by DORA.

II. SCOPE OF APPLICATION

- DORA applies to a broad spectrum of 'financial entities'. This includes (i) credit institutions, (ii) payment institutions, (iii) account information service providers, (iv) electronic money institutions, (v) investment firms, (vi) crypto-asset service providers and issuers of asset-referenced tokens, (vii) central securities depositories, (viii) central counterparties, (ix) trading venues, (x) trade repositories, (xi) managers of alternative investment funds, (xii) management companies, (xiii) data reporting service providers, (xiv) **insurance and reinsurance undertakings**, (xv) **insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries**, (xvi) **institutions for occupational retirement provision**, (xvii) credit rating agencies, (xviii) administrators of critical benchmarks, (xix) crowdfunding service providers, and (xx) securitisation repositories[1].

- In addition, DORA applies to **critical ICT third-party service providers**, i.e., certain undertakings providing ICT services (to financial entities)[2].

- DORA exempts from its scope of application certain financial entities due to their size. For example, insurance and reinsurance undertakings exempted from compliance with Solvency II shall also be exempted from compliance with DORA[3]. Also, DORA does not apply to insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises[4] nor to institutions for occupational retirement provision which operate pension schemes which together do not have more than fifteen (15) members in total[5].

III. PROPORTIONALITY

Given the broad scope of application of DORA and the extensive obligations it imposes on financial entities, DORA introduces the so-called '**proportionality principle**'[6].

[1] Art. 2 (1) DORA.
[2] Art. 2 (1) (u) DORA.
[3] Art. 2 (3) (b) DORA.
[4] Art. 2 (3) (e) DORA.
[5] Art. 2 (3) (c) DORA.
[6] Art. 4 DORA.

According to the proportionality principle, financial entities must implement the rules laid down in Chapter II of DORA in accordance with the principle of proportionality, considering their size and overall risk profile, and the nature, scale and complexity of their services, activities, and operations.

In addition, the application by financial entities of Chapters III, IV and V, Section I, of DORA must be proportionate to their size and overall risk profile, and to the nature, scale and complexity of their services, activities, and operations, **as specifically provided for in the relevant rules of those Chapters**.

The competent authorities must consider the application of the proportionality principle by financial entities when reviewing the consistency of the ICT risk management framework based on the reports submitted upon the request of competent authorities.

IV. OBLIGATIONS OF FINANCIAL ENTITIES

The main obligations of financial entities under DORA are set out in Chapters II, III, IV, and V, Section I of DORA[7] and relate to (i) ICT risk management (Chapter II); (ii) ICT-related incident management, classification and reporting (Chapter III); (iii) digital operational resilience testing (Chapter IV); and (iv) managing ICT third-party risk (Chapter V, Section I). Below, we will briefly introduce the main obligations of financial entities in respect of each of the above topics.

ICT Risk Management

- Chapter II of DORA obliges financial entities to put in place an **internal governance and control framework** that ensures an effective and prudent management of ICT risk to achieve a high level of digital operational resilience.

- Extensive obligations are imposed on the financial entity's '**management body**'[8], which bears the ultimate responsibility for the management of the financial entity's ICT risk and, more generally, plays a crucial role in compliance with DORA[9]. In respect of ICT third-party risk, financial entities must appoint an 'ICT Third-Party Officer' to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services or must designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.

- Financial entities must 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 comprehensively and to ensure a high level of digital operational resilience. The elements that the ICT risk management framework must comprise, are set out in more detail in DORA. The ICT risk management framework must include, amongst others, a digital operational resilience strategy setting out how the framework shall be implemented[10].

- The requirements for the ICT risk management framework centre on specific functions in ICT risk management, namely (i) identification[11], (ii) protection and prevention[12], (iii) detection[13], (iv) response and recovery[14], (v) learning and evolving[15] and (vi) communication[16].

- The European Supervisory Authorities (ESAs) are mandated to develop, in consultation with the European Union Agency on Cybersecurity (ENISA) common **draft regulatory technical standards** further detailing the requirements to be met by financial entities' ICT risk management framework by 17 January 2024. Power is delegated to the Commission to adopt such regulatory technical standards.

- Finally, it should be noted that certain types of (smaller) financial entities are subject to a simplified ICT risk management framework[17].

[7] Art. 5 through 30 DORA.
[8] 'Management body' refers to a management body as defined in Article 4(1), point (36), of Directive 2014/65/EU, Article 3(1), point (7), of Directive 2013/36/EU, Article 2(1), point (s), of Directive 2009/65/EC of the European Parliament and of the Council (31), Article 2(1), point (45), of Regulation (EU) No 909/2014, Article 3(1), point (20), of Regulation (EU) 2016/1011, and in the relevant provision of the Regulation on markets in crypto-assets, or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national law.
[9] Art. 5 DORA.
[10] Art. 6 DORA.
[11] Art. 8 DORA.
[12] Art. 9 DORA.
[13] Art. 10 DORA.
[14] Art. 11 and 12 DORA.
[15] Art. 13 DORA.
[16] Art. 14 DORA.
17 Art. 16 DORA.

ICT-related incident management, classification, and reporting

- Chapter III of DORA contains requirements for financial entities with respect to the **management** and **classification** of **ICT-related incidents and cyber threats**[18] as well as the **reporting**[19] of ICT-related incidents.

- Financial entities will be obliged to report **major ICT-related incidents** to the competent authorities. DORA further provides for a possibility for financial entities to notify, on a voluntary basis, significant cyber threats to the competent authorities.

- The ESAs are – again – mandated to develop, in consultation with the ECB and ENISA, common **draft regulatory technical standards** further specifying certain requirements in relation to the classification and reporting of ICT-related incidents by 17 January 2024. The ESAs, in consultation with the ECB and ENISA, must also prepare common draft regulatory technical standards aiming at **harmonising** the reporting content and templates. Power is delegated to the Commission to adopt such regulatory technical standards.

Digital operational resilience testing

- Chapter IV of DORA sets out requirements for **digital operational resilience testing**, i.e., periodically addressing cyber resilience and identifying weaknesses, deficiencies, or gaps, as well as the prompt implementation of corrective measures[20].

- Financial entities must establish, maintain, and review a sound and comprehensive digital operational resilience **testing programme** as an integral part of their ICT risk management framework. The digital operational resilience testing programme must provide for the execution of appropriate tests, such as vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing, and penetration testing[21].

- In addition, financial entities identified by competent authorities as '**significant**' will be required to conduct advanced Threat-Led Penetration Tests (TLPT)[22]. TLPT is a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, which delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems.

Managing ICT third-party risk

- Chapter V, Section I of DORA imposes obligations on financial entities to ensure the sound management of ICT third-party risk. Financial entities will be required to manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework[23].

- As part of their ICT risk management framework, financial entities must adopt, and regularly review, a **strategy on ICT third-party risk**, considering the multi-vendor strategy, where applicable. The strategy on ICT third-party risk must include a policy on the use of ICT services supporting **critical** or **important functions** provided by ICT third-party service providers and must apply on an individual basis and, where relevant, on a sub-consolidated and consolidated basis.

  The management body must, based on an assessment of the overall risk profile of the financial entity and the scale and complexity of the business services, regularly review the risks identified in respect to contractual arrangements on the use of ICT services supporting critical or important functions[24].

- Financial entities must inform the competent authority in a timely manner about any planned contractual arrangement on the use of ICT services supporting **critical** or **important functions** as well as when a function has become critical or important.

[18] Art. 18 DORA.
[19] Art. 19 DORA.
[20] Art. 24 through 27 DORA.
[21] Art. 25 DORA.
[22] Art. 26 DORA.
[23] Art. 28 (1) DORA.
[24] Art. 28 (2) DORA.

- DORA also contains specific requirements with respect to the **contractual arrangements**[25] entered into between financial entities and ICT third-party service providers and obliges financial entities to **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[26].

V. Oversight Framework for Critical ICT Third Party Service Providers

- DORA creates **an entirely new oversight framework for critical ICT third-party service providers**[27].

- Following an assessment, the ESAs will designate the ICT third-party service providers that are **critical** for financial entities and appoint, for each critical ICT third-party service provider, an ESA that shall function as 'Lead Overseer'[28].

  The **criteria** for designation of an ICT third-party service provider as a **critical** ICT third-party service provider are laid down in Art. 31 (2) DORA and includes criteria such as (i) the systemic impact on the stability, continuity or quality of the provision of financial services in the event that the relevant ICT third-party service provider would face a large scale operational failure, (ii) the systemic character or importance of the financial entities that rely on the relevant ICT third-party service provider, (iii) the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider, and (iv) the degree of substitutability of the ICT third-party service provider.

- Critical ICT third-party service providers will be subject to **comprehensive oversight** from their Lead Overseer, together with an 'Oversight Forum' established as a sub-committee of the Joint Committee of the ESAs.

  The Lead Overseer's main task is to assess whether each critical ICT third-party service provider has in place **comprehensive, sound, and effective rules, procedures, mechanisms, and arrangements to manage the ICT risk** which it may pose to financial entities. The assessment will focus mainly on ICT services provided by the critical ICT third-party service provider supporting the critical or important functions of financial entities. However, where necessary to address all relevant risks, that assessment shall extend to ICT services supporting functions other than those that are critical or important[29].

- The powers of the Lead Overseer include (i) requesting all relevant information and documentation[30], (ii) conducting general investigations[31], (iii) conducting inspections[32], (iv) issuing recommendations and (v) requesting, after the completion of the oversight activities, reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service providers in relation to the recommendations made.

- Critical ICT third-party service providers will be due **oversight fees** that fully cover the Lead Overseer's necessary expenditure in relation to the conduct of oversight tasks pursuant to DORA. The amount of the fee charged to a critical ICT third-party service provider will cover all costs derived from the performance of the duties set out in Section II of Chapter V of DORA and must be proportionate to its turnover[33].

VI. Information-sharing arrangements

To support financial entities' defensive capabilities and threat detection techniques, DORA explicitly allows financial entities to set up **cyber threat information and intelligence exchange arrangements** among themselves. This includes exchanging information on indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools. Financial entities must notify competent authorities of their participation in the information-sharing arrangements, upon validation of their membership, or, as applicable, of the cessation of their membership, once it takes effect.

25 Art. 30 DORA.
26 Art. 28 (3), 3rd para.
27 Chapter V, Section II DORA.
28 Art. 31 (1) DORA.
29 Art. 33 (2) DORA.
30 Art. 37 DORA.
31 Art. 38 DORA.
32 Art. 39 DORA.
33 Art. 43 DORA.

VII. Delegated Acts

DORA confers on the Commission the power to adopt delegated acts. As already stated above, the European Supervisory Authorities (ESAs) are mandated to develop common draft regulatory technical standards on various topics by 17 January 2024. Power is delegated to the Commission to adopt such regulatory technical standards.

VIII. Entry-into-force, Timeline and Application

DORA has entered into force on the twentieth (20th) day following that of its publication in the Official Journal of the European Union (i.e., 11 January 2023) and shall apply from 17 January 2025.

Hence, financial entities and other relevant stakeholders (e.g., competent authorities and (critical) ICT third party service providers) are granted a transition period of **two (2) years** to prepare for DORA's entry-into-force.

Importantly, various delegated acts and regulatory technical standards are expected to be published by the Commission in the period between 17 January 2024 and 17 January 2025, i.e., DORA's date of application.

IX. Checklist

Lydian's Information & Communication Technology (ICT) team has prepared a detailed checklist of the requirements financial entities – including insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, and institutions for occupational retirement provision – must meet to comply with DORA. If you would like to receive our checklist, please e-mail marketing@lydian.be. The checklist is provided free of charge.

Do not hesitate to contact Lydian's *Information & Communication Technology (ICT)* team in case of questions and/or should you require assistance in respect of the implementation of DORA within your organisation.

LYDIAN ANTWERP
Arenbergstraat 23
2000 Antwerp
Belgium
T +32 (0)3 304 90 00
F +32 (0)3 304 90 19

LYDIAN BRUSSELS
Tour & Taxis
Havenlaan 86C/b113
1000 Brussels
Belgium
T +32 (0)2 787 90 00
F +32 (0) 2 787 90 99

LYDIAN HASSELT
Thonissenlaan 75
3500 Hasselt
Belgium
T +32 (0) 11 260 050
F +32 (0) 11 260 059