KPMG

Financial Risk&Regulation

The DORA Regulation sets harmonised expectations for a wide range of financial operators

Newsletter – 2023. September

The 2022/2554 EU regulation[1] (hereinafter: DORA) – has been entered into effect on 16th January 2023. and applicable from 17th January 2025. – focuses on managing the cyber risks of financial institutions and strengthening their digital resilience along common principles. With implementing the DORA regulation and the regulation package, not only the operation security can be increased but also the consumer confidence, as well as the effectiveness of cross-border services.

Background

The financial system's information, communication and technological (ICT) systems' connectedness and mutual dependencies result by to that from the vulnerability arising from institution may cause difficulties affecting the functioning of all the institutions of the European Union and with this may can also affect investor's confidence in the financial system, which may be led to banking panic.[2]

The DORA intends to introduce a harmonised set of cybersecurity requirements to prevent these situations, which – with the size and operation of the institution – are **based on a proportional and risk-based approach**, also defines a new digital operational risk management framework concerning financial sector operators and each ICT service providers, which is specifically aimed at promoting digital resilience. Its significance is that, although it builds on previously expected, established risk management activities (as EU e.g., NIS and NIS 2 directives[3], all member states requirements, international ICT standards and recommendations, e.g. EBA/ESMA/EIOPA guidelines and the recommendations of member state authorities transposing them), however, this is the first comprehensive regulation which sets coherent and harmonised requirements for a wide range of financial sector operators at EU level.

DORA applies two approaches: on one hand, it sets rules for financial institutions, and on the other hand, it also regulates the activities of companies that provide third-party technology services (ICT suppliers) to financial institutions. It considers the size, activities and business profile of the financial institution and determines what IT risk management requirements must met in accordance to these.

The subject scope of the regulation

The subject scope of the regulation covers basically the whole range of banking and neo banking activities, extends to all the financial service providers and their ICT suppliers (whether or not it counts as outsourcing under sectoral legislation), because the increased risks arising from digitalisation may be observed in particularly these services. E.g. an electronic money issuer applies video customer identification to its service, using an external service provider, to whose system the

1 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
2 https://www.consilium.europa.eu/en/policies/cybersecurity/
3 DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

issuer connects its own system. In the case of vulnerabilities in a cloud-based system for example, a large amount of personal data, including the facial image, sound recording, and personal identification data of natural persons, as well as the banking and payment secrecy associated with them, could get into the hands of unauthorised persons, or the electronic money issuer's own systems may become jeopardized through this system, compromising even more personal data and banking secrecy.

Relevant suppliers of the financial service providers listed above may include e.g., cloud service providers; software development, support or digital service providers (e.g., data analytics, data centre, automatic decision making, data processing), however, the hardware providers, electric telecommunications service providers, such as telephone and internet service providers do not fall under the subject scope of the regulation. Microenterprises, smaller institutions under certain sectoral legislation, and institutions exempted and excluded from the scope by a member state are exempt from the above-mentioned rules.

Although certain clarifying questions remain to be answered on the scope of DORA (does not name certain types of institutions, e.g. private pension funds), the anticipation is that the subject scope will be widely interpreted and will probably include operators widely.

Regulated areas

The main regulatory areas covered by the DORA regulation organised into 5 pillars and a corporate governance block:

- ICT risk management requirements.
- Testing of digital operational resilience.
- Management of ICT risks arising from third-parties, contracts, and their supervision (supervision framework).
- Reporting on notifications (announcement of significant ICT events and voluntary authority notifications of significant cyber threats, authority notifications of payment-related operational or security events).

Information sharing (cyber threats and vulnerability related information sharing). In addition to the field of corporate governance, it also sets rules on the management bodies and on the management requirements for managers).

Framework built on previous expectations

One of the most important requirements of DORA – although that's not exactly new -, that it expects a robust, comprehensive, and well-documented ICT risk management framework to be developed and integrated into the company's risk management system from the operators. With this implemented framework the financial institutions must minimise the impact of ICT risks. The compliance with this is monitored by an independent control function within the organisation.

New element added to the legislation, that the risk management frameworks must include a **specific strategy for digital operational resilience, with concrete objectives and methods**.

Financial organisations must maintain up to date ICT systems, -protocols and -tools, which are proportional, reliable and have sufficient capacity, and resilient in market stress situations or in other adverse situations.

After introducing the strategy, must be followed by **security measures** reducing and managing risks. Financial organisations are necessary to apply processes and solutions which guarantee the security of data transfer devices, minimise the data damage and loss, unauthorised access, and also the risk of technical failures that could disrupt business operations, block incidents concerning data (availability, authenticity, integrity and compromised confidentiality), and the risk management of data manage, including human risks too.

Financial organisations must develop a process for **detecting, managing, and reporting** ICT-related events. Firstly, they must register all significant ICT incidents and cyber threats and classify them according to a set of criteria, secondly, they must establish appropriate monitoring procedures.

A **comprehensive process must be developed for testing** of operating resilience. As a result, readiness to handle ICT-related events can be evaluated, the strengths and gaps of digital operational resilience become identifiable. The tests must be carried out annually, by an independent internal or external party through all systems that supports key functions.

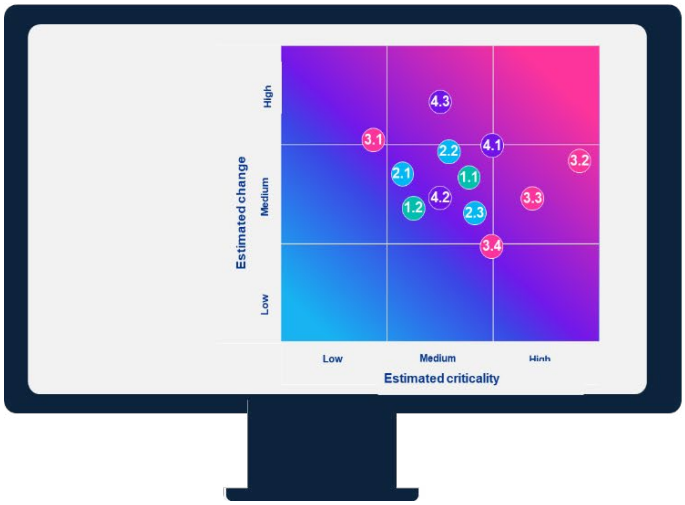
DORA pays particular attention to **(third party) managing ICT suppliers' risks**. It harmonises the rules and sets new rules for key suppliers. Which supplier is considered a key service provider is defined by the supervisory authority, but mainly the critical or important function supporting ICT services may fall under this category. The supervisory authority for these service providers prepares an individual supervision plan to the service provider, registers them, and has control rights.

In determining which service providers are key, the supervisory authority will consider a number of criteria: for example, consider potential systemic impacts, which occur in the event of a failure of the service provider, and the environment of service provision, such as the user organisations (their number, character, interconnection, substitutability of their services) and the number of member states involved.

The Hungarian market operators have already previously met some of the requirements in various guidelines, MNB recommendations, but those level of implementation were realized differently. Larger and more complex operation and size, regardless of the complexity of the existing legislation, companies that are not entirely in line with regulatory requirements and market standards may need to initiate a more resource-intensive project to achieve DORA's expected resilience level. It is also important to emphasize that the task is not only the financial institutions' own compliance. For financial institutions (e.g. banks and insurance companies) working with many ICT suppliers, it is high priority, that their suppliers also start the compliance process and make the necessary changes on their side.

Our services related to DORA regulation

The regulation is applicable from 17th January 2025., but it is recommended to give time for preparation. Some of the topics will be clarified and detailed by several RTS and ITS, which are now only in the consultation phase or not yet in the planning phase. Until these details are available, the preparation extends to the general rules of DORA, and the compliance assessment of the already existing ESA (and MNB) recommendations, possible gaps and actions can be roughly identified without knowing the detailed rules. In case of large financial groups, the assessment can also be launched, that aims to determine what elements of the DORA require central implementation, and which has flexibility or task at domestic level. Early preparation is also necessary because several areas of expertise (operational risk management, IT risk management, procurement, process control, legal, compliance, etc…) requires coordinated work. With these preparatory steps, the institution will be able to begin the detailed implementation project with a good level of compliance after the publication of RTSs and ITSs.



ICT Risk Management, Governance & Strategy

- 1.1 Digital Operational Resilience Strategy (Art. 6)
- 1.2 Responsibility of the governing body (Art. 5)

Digital operational resilience

- 2.1 Threat-based penetration tests (Art. 26-27)
- 2.2 Testing digital operational resilience (Art. 24-25)
- 2.3 Testing of the recovery plans (Art. 11)

Management of ICT third-party risks

- 3.1 ICT third-party strategy (Art. 28)
- 3.2 Contract supplements and risk analysis (Art. 28, 30)
- 3.3 Information Register (Art. 28)
- 3.4 Exit strategies (Art. 28, 30)

ICT incident reporting

- 4.1 Detection, classification and reporting of incidents (Art. 10, Art. 17-19)
- 4.2 Response to ICT incidents (Art. 11)
- 4.3 Communication (Art. 11 & 14)

The text of DORA regulation (without the RTSs) and the estimated impact to the operation of financial institutions based on initial preparation experience. Factual impacts may differ for each institution, so they must be examined individually.

An important factor of compliance with the regulation is to conduct the security investigations, details of further information can be found on the following pages: Digital Operational Resilience Act - KPMG Hungary, Cyber security advisory - KPMG Hungary

---

The newsletter was prepared by: Viktória Glózer-Say and Kamilla Kátai.

Contacts:

Ágnes Rakó
Partner
M: +36 70 370 1792
E: agnes.rako@kpmg.hu

Kornél Lukács
Partner
M: +36 70 977 6564
E: kornel.lukacs@kpmg.hu

Péter Szalai
Associate Partner
M: +36 70 370 1739
E: peter.szalai@kpmg.hu

Gergő Wieder
Director
M: +36 70 333 1471
E: gergo.wieder@kpmg.hu

Viktória Glózer-Say
Manager
M: +36 70 978 7031
E: viktoria.glozer-say@kpmg.hu

KPMG.hu