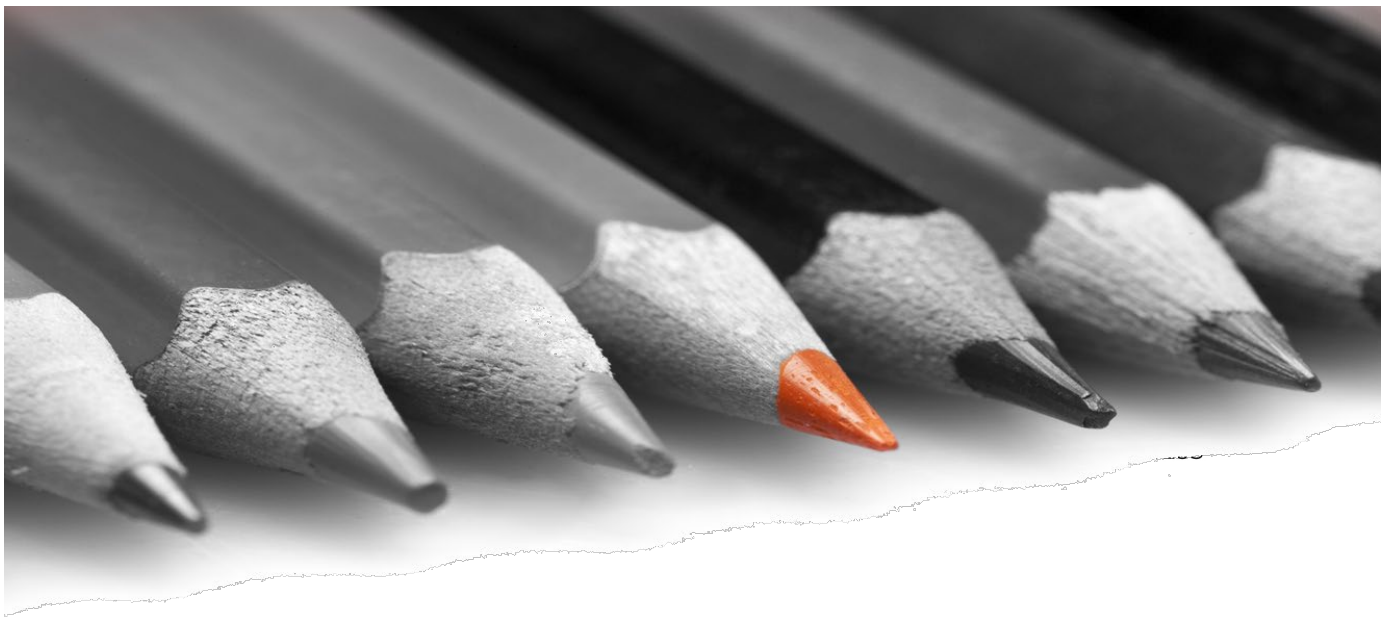

MPR PARTNERS

DORA – A NEW CHAPTER FOR THE FINANCIAL AND ICT SECTORS

1. Background

In December 2022, the European Parliament and the Council adopted Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) no. 1006/2009, (EU) no. 648/2012, (EU) no. 600/2014, (EU) no. 909/2014 and (EU) 2016/1011 (the "**Digital Operational Resilience Act**" or "**DORA**").

DORA, which shall apply starting with January 17, 2025, aims to achieve a high level of digital operational resilience for regulated financial entities and shall apply to the following categories of such entities (hereinafter collectively referred to as "**Financial Entities**"):

(i) credit institutions;

(ii) payment institutions;

(iii) account information service providers;

(iv) electronic money institutions;

(v) investment firms;

(vi) crypto-assets service providers;

(vii) central securities depositaries;

(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 services providers;

(xx) securitisation repositories.

In addition to all of the above, DORA shall apply and influence the activity of information and communication technology third-party service providers ("**ICT Third Party Service Providers**").

In the sections below, we will detail the main aspects stemming from DORA's provisions that affect Financial Entities and ICT Third Party Service Providers.

2. Uniform requirements

In order to achieve its afore-mentioned purpose, DORA lays down uniform requirements for the security of network and information systems supporting the business process of Financial Entities, including:

- requirements applicable to Financial Entities as regards:
  - (i) information and communication technology ("**ICT**") risk management;
  - (ii) reporting of major ICT-related incidents;
  - (iii) measures for sound management of ICT third-party risk.

- requirements in relation to the contractual arrangements concluded between Financial Entities and ICT Third Party Service Providers;

We will highlight the main obligations imposed on Financial Entities and ICT Third Party Service Providers in the subsequent sections.

3. Governance and organisation

DORA requires Financial Entities to have in place an internal governance and control framework that ensures "*an effective and prudent management of ICT risk*".

Such requirement must be achieved by the Financial Institution's management body (whom, per the regulation, bears the ultimate responsibility for managing the Financial Entity's ICT risk), whom, to this end, must implement a large set of measures, such as:

(i) put in place policies aiming to ensure the maintenance of high standards of data availability, authenticity, integrity and confidentiality;

(ii) approve, oversee and review the implementation of the Financial Entity's business continuity policy and ICT response and recovery plans;

(iii) approve and review the Financial Entity's ICT internal audit plans, ICT audits and material amendments thereof;

(iv) allocate and review the budget required to fulfil the Financial Entity's digital operational resilience needs;

(v) approve and review policies on arrangements regarding the use of services provided by ICT Third Party Service Providers;

(vi) put in place reporting channels enabling it to be informed on arrangements with ICT Third Party Service Providers, amendments thereto and impact of such amendments.

4. ICT risk management framework

Per DORA, Financial Entities shall also be required to implement an ICT risk management framework (which needs to be documented and reviewed at least yearly) as part of their overall risk management system enabling them to address ICT risk quickly, efficiently and comprehensively, comprising of at least:

(i) strategies;

(ii) policies;

(iii) procedures;

(iv) ICT protocols and tools.

Responsibility for managing and overseeing ICT risk shall be assigned to a dedicated control function that shall have an appropriate level of independence in order to avoid conflicts of interest.

Financial Entities' ICT risk management framework shall also include a digital operational resilience strategy including methods to address ICT risk and achieve ICT objectives, by, amongst others:

(i) explaining how the ICT risk management framework supports the Financial Entity's business strategy and objectives;

(ii) establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the Financial Entity, and analysing the impact tolerance for ICT disruptions;

(iii) setting out clear information security objectives, including key performance indicators and key risk metrics;

(iv) outlining the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it;

(v) implementing digital operational resilience testing.

5. Protection and prevention

Financial Entities must monitor and control the security of ICT systems in order to prevent/minimize the impact of ICT risks. To this end, besides having in place suitable ICT security policies, procedures, protocols and tools, Financial Entities shall also be required to use ICT solutions and processes that meet the following requirements:

(i) ensure the security of the means of transfer of data;

(ii) minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity;

(iii) prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data;

(iv) ensure that data is protected from risks arising from data management, including poor administration, processing- related risks and human error.

6. Incident management

Besides prevention and protection against ICT risks/incidents, Financial Entities shall be required to have in place an ICT-related incident management process aimed to detect, manage and notify ICT-related incidents.

All such incidents and significant cyber threats shall be recorded and appropriate procedures and process to monitor, handle and follow-up on such incidents must be also implemented.

The ICT-related management process shall, amongst others:

(i) put in place early warning indicators;

(ii) establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and severity and according to the criticality of the services impacted;

(iii) assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;

(iv) set out plans for communication to staff, external stakeholders and media and clients;

(v) ensure that at least major ICT-related incidents are reported to relevant senior management and inform the management body of at least major ICT-related incidents;

(vi) establish ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner.

ICT-related incidents shall need to be classified by Financial Entities and their impact established by the same based on various criteria.

All ICT-related incidents classified as major shall be reported to the competent national authorities. Such report shall contain all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts.

Where established that the major-ICT related incident has an impact on the financial interests of clients, Financial Entities shall also, without undue delay as soon as they become aware, inform the clients accordingly, including as regards the measures taken to mitigate the adverse effects.

7. Management of ICT third-party risk

Perhaps most important from a legal and business perspective, DORA imposes monitoring of ICT risks resulting from Financial Entities' relationship with ICT Third Party Service Providers.

To this end, Financial Entities will be required to set up, maintain and update a register of information on all contractual arrangements on the use of ICT services provided by ICT Third Party Service Providers.

In addition, prior to engaging in a contractual arrangement with ICT Third Party Service Providers, Financial Entities must asses a number of aspects, such as:

(i) whether the contractual arrangement covers the use of ICT services supporting a critical or important function;

(ii) undertake all due diligence on prospective ICT Third Party Service Providers and ensure throughout the selection and assessment process that the same is suitable.

DORA also includes obligations that shall impact the clauses of contractual arrangements between Financial Entities and ICT Third Party Service Providers, as the same must allow the Financial Entities to terminate such arrangements in various scenarios, including as a result of the ICT Third Party Service Providers' weaknesses to their overall ICT risk management.

Such contractual arrangement must also include various additional clauses required under DORA, such as:

(i) a clear and complete description of all functions and ICT services to be provided by the ICT Third Party Service Providers;

(ii) locations where the contracted functions and ICT services are provided and where data is processed;

(iii) provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the Financial Entity in the event of the insolvency, resolution or discontinuation of the business;

(iv) the obligation of the ICT Third Party Service Provider to provide assistance to the Financial Entity at no additional cost, or at a cost that is determined ex-ante, when an ICT incident that is related to the ICT service provided occurs;

(v) the obligation of the ICT Third Party Service Provider to fully cooperate with the competent authorities.

8. Conclusions

DORA will impact both Financial Entities and ICT Third Party Service Providers, both from a technical and contractual perspective.

In order to comply with the DORA requirements by the time the same shall apply (starting with January 17, 2025), Financial Entities and ICT Third Party Service Providers will arguably require to assess (preferably together) currently used ICT systems, perform gap analysis and adjust contractual arrangements.

Therefore, both technical and legal assistance will be likely required in order for DORA affected entities to properly prepare for the implementation of DORA.

Daniel Alexie

Partner

daniel.alexie@mprpartners.com