New European Regulation on the digital operational resilience of the financial sector (DORA)

CMS Albiñana & Suárez de Lezo

31 January 2023

NEW EUROPEAN REGULATION ON THE DIGITAL OPERATIONAL RESILIENCE OF THE FINANCIAL SECTOR (DORA)

On 27 December 2022, Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 and (EU) 2016/1011 (the '**Regulation**' or '**DORA'**) was published in the Official Journal of the European Union.

The Regulation was published along with Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 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 regarding digital operational resilience of the financial sector (the '**Directive'**).

Both aim to achieve a high level of common digital operational resilience, as defined in the Regulation and detailed below, by establishing standard requirements for network security and information systems that are the support structure for the business processes of financial entities.

EU countries already have operational risk regulations in place. However, gaps have been identified, making it necessary to further define guidelines on protection, detection, containment, recovery and repair of information and communication technology ('**ICT'**) incidents, following reports of such risks or regarding digital evidence. The Regulation fills these gaps by laying down specific rules on risk management, incident reporting, operational resilience testing and risk monitoring when they involve third parties.

1. SCOPE AND PURPOSE

All financial entities are bound by the Regulation, with certain exclusions. Therefore, a wide range of entities are covered: credit, payment, electronic money or investment services institutions, alternative investment fund managers, crypto-asset service providers, insurance and reinsurance companies and intermediaries, credit rating agencies, providers of equity finance services or securitisation registers, among others.

The main development regarding the scope of application is that third-party ICT services providers will also be subject to monitoring under the Regulation. These companies offer major support for financial entities in the European system and their services are essential. It is therefore of upmost importance to assess and monitor the rules, procedures, and mechanisms they have in place to manage ICT risks and their impact on financial entities. The Regulation defines an ICT risk as '*any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the network and information systems, of any technology dependent tool or process, of operations and processes, or the provision of services, by producing adverse effects in the digital or physical environment'*.

The Regulation aims to achieve an adequate level of digital operational resilience common to all EU Member States. The text defines digital operational resilience as '*the ability of a financial entity to build, secure and review its operational integrity and reliability by ensuring either, directly or indirectly through the use of services provided by third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses and which support the continued provision of financial services and their quality, including throughout disruptions*'.

The Regulation sets out rules on the processes of such entities and, in particular, lays down requirements applicable to financial entities and requirements regarding contractual arrangements between third-party ICT service providers and financial entities. It also regulates the supervisory framework for critical third-party ICT service providers during the provision of services to financial entities.

2. REQUIREMENTS FOR FINANCIAL ENTITIES

In order to support ICT-related risk management, a solid, quick, efficient, and comprehensive framework has been launched to ensure a high level of digital operational resilience. This framework should include all procedures or tools used to protect information and ICT assets (such as software, hardware, or servers, as well as data centres or other types of infrastructure). Financial entities should continuously monitor and control the security and operation of systems and tools, with mechanisms in place to detect unusual activity and implement an ICT business continuity policy, to ensure the financial entity may continue operating.

Financial entities must also keep a record of ICT-related incidents or significant cyber threats, classifying them and detailing their impact, following what is required by the Regulation. This applies to payment-related operational or security incidents involving credit, payment or e-money institutions and account information service providers. Serious incidents must also be reported to the authorities. Reporting obligations may be outsourced to third-party service providers.

To assess digital operational resilience, financial entities, except micro-enterprises, must set up, maintain, and regularly review a comprehensive testing programme, as part of the ICT risk management framework. The programme must review any specific risks to which the entity may be exposed as well as any other relevant factors. Certain entities, due to their size and the potential consequences of defects or bugs in their system, will have to conduct advanced threat-based penetration testing, at least every three years, carried out by skilled, qualified, and certified testers, as may be required by the Regulation.

The Regulation also allows entities to exchange information and intelligence on cyber threats and related vulnerabilities, if they are aimed at improving digital operational resilience, they take place within trusted circles of entities, and agreements are drafted to ensure that such exchanges, trade secrets, personal data and competition policies are protected. This arrangement will allow the

financial sector to collectively respond to threats, limiting their reach and spread through the different financial channels.

3. REQUIREMENTS ON CONTRACTUAL ARRANGEMENTS BETWEEN THIRD-PARTY ICT SERVICE PROVIDERS AND FINANCIAL ENTITIES

One of the most relevant sections of the Regulation introduces measures to manage ICT-related risks arising from third parties, especially when financial entities rely on third party ICT service providers to support critical or important business functions. A critical or important function is defined as 'a *disruption which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation*'.

Despite the existence of the 2019 European Banking Authority (EBA) Guidelines on outsourcing and the 2021 European Securities Markets Authority (ESMA) Guidelines on outsourcing to cloud service providers, EU law does not thoroughly address systemic risk management that may be triggered in the financial sector by the entry of third-party ICT service providers, nor does it shed light on how to understand or carry out adequate monitoring of such ICT-related risks.

To this end, it is crucial that the engagement between the entity and the third party is set out in a written agreement, outlining the rights and obligations of both parties in an abiding and accessible format. The aim is to create a minimum safeguard and for financial entities to monitor all ICT-related risks that may arise from the service provider. As the Regulation notes, these requirements are to complete the sector-specific legislation applicable to outsourcing.

The Regulation also points out aspects that, regardless of whether or not the function is considered critical or important, must be included in the agreements signed between financial entities and third-party ICT service providers. When they are considered critical or important, the requirements set out in the Regulation are stricter.

4. ESTABLISHMENT AND IMPLEMENTATION OF THE SUPERVISORY FRAMEWORK FOR ESSENTIAL THIRD-PARTY ICT SERVICE PROVIDERS DURING THE PROVISION OF SERVICES TO FINANCIAL ENTITIES

Finally, the Regulation also creates a framework for the supervision of critical third-party ICT service providers to follow-up on their activities, ensuring that the provision of ICT services is subject to the same regulatory framework as if they were carried out internally by the financial entity.

The European Supervisory Authorities, through the Joint Committee and upon recommendation of the Supervisory Forum, will assess what third-party ICT service providers are considered critical, taking into account:

(i) the systemic impact on the stability, continuity, or quality of the provision of financial services in the event that the ICT service provider were to face a large-scale operational failure to provide its services;

(ii) the systemic character or importance of the financial entities that rely on the provider, assessed from the number of globally significant institutions or other entities that rely on the provider, and the interdependence between them and other financial entities;

(iii) the financial entity's reliance on the services provided in relation to critical or important functions that ultimately involve the same service provider, irrespective of whether financial entities rely on these services directly or indirectly, through subcontracting arrangements; and

(iv) the degree of substitutability of the service provider, taking into account the lack of real alternatives or difficulties to partially or fully migrate the relevant data and workload from the service provider to a different company.

They must also appoint a European Supervisory Authority as 'Lead Overseer' for each critical third-party ICT service provider.

5. ENTRY INTO FORCE AND IMPLEMENTATION

Both the DORA Regulation and the Directive entered into force on 17 January 2023, the former will be directly applicable as of 17 January 2025.

Ricardo Plasencia
CMS Partner
Financial Markets and Services
T +34 91 187 19 13
E ricardo.plasencia@cms-asl.com

Lucía Escauriaza
CMS Associate
Financial Markets and Services
T +34 91 451 93 35
E lucia.escauriaza@cms-asl.com