Deloitte.

Regulatory News Alert

EU Digital Operation Resilience Act passed: implications for the financial sector

November 16th, 2022

In summary:

- In the plenary session of the European Parliament on Nov. 10, final agreement was reached on the Digital Operational Resilience Act (DORA). This is the most important EU-wide regulatory initiative on operational resilience and cybersecurity in the Financial Services (FS) sector and represents a major step toward consolidating and evolving regulatory requirements for market participants in the ICT field.
- DORA requires practitioners to adopt a broader corporate view of resilience, with clear responsibilities strengthened for Corporate Bodies and top management; it applies to the majority of financial sector operators operating in the EU, and establishes binding rules for ICT risk management, incident reporting, resilience testing, and third-party risk management (TPRM).
- DORA is also the world's first regulatory framework for FS supervisors to oversee critical ICT service providers (CTPPs), including cloud service providers (CSPs).
- The Regulation provides financial sector operators with a basis for directing the implementation phase. Practitioners are therefore required to conduct an impact analysis aimed at identifying gaps and evolutionary areas on which to develop a roadmap for implementing a strong operational resilience framework by Q4 2024, in line with the new requirements.
- DORA is not just a regulatory requirement, but a true accelerator in the evolutionary process of digital risk management systems, as well as an opportunity for financial sector operators to enhance the level of understanding and assessment of the impact of operational incidents/disruptions on their business and customers.

  This analysis, conducted by the Deloitte Centre for Regulatory Strategy, with insight from Deloitte experts from across Europe, delves into the significant changes and potential challenges that practitioners will face in implementing the five pillars of DORA.

Overview

Following extensive negotiations at the EU level, a comprehensive technical agreement on the DORA regulation was achieved, andthe administrative process is just a short time away from being closed with publication in the Official Journal of the EU. The full text of the regulation has already been published by the European Parliament, and financial industry players must now begin to assess its impacts on their

business, organizational and operational models. We believe that DORA will represent a "game changer" that will push financial services operators to fully understand how their current management practices in ICT Risk, Cyber and Third-Party Risk Management impact the level of resilience of their most critical functions, pushing towards the development of entirely new operational resilience capabilities, such as advanced risk scenario testing methodologies.
Operators in the financial sector will have a relatively tight 24-month period to comply with the new regulatory standards. The implementation period will begin 20 days after publication in the EU Official Journal (scheduled for November 2022). This means that, by the fourth quarter of 2024, relevant supervisors will expect industry entities to be fully compliant with the new DORA requirements, including the provisions that will be contained in the Level 2 regulations to be set by the European regulators (see Part II below).

Part I: What are the implications of the new DORA regulation for financial sector operators?

The approved version of the DORA regulation confirms the five basic pillars of the European Commission's initial proposal. From Deloitte's analysis of the text of the final technical agreement, the following main implications emerge:

1. ICT risk management – focus on critical business functions

DORA gives a pivotal role to the organisational management body by giving it "full responsibility" in adopting, managing and monitoring the digital operational resilience strategy; managing ICT risks; and reviewing and approving the corporate policy on the use of ICT Third Party Providers (TPPs). It also strengthens the role and responsibilities of internal ICT functions. Furthermore, DORA empowers the relevant authorities to apply administrative sanctions and corrective measures to members of the management body for any violation of the regulation.

DORA's ICT risk management requirements are consistent with the European Banking Authority's (EBA) guidelines on ICT security and risk management (EBA/GL/2019/04) and the European Insurance and Occupational Pensions Authority's (EIOPA) guidelines on ICT security and governance (EIOPA-BoS-20/600), while also strengthening their scope and related supervisory approach. In addition, the binding nature of the regulation and its new requirements, falling within the scope of primary legislation, will intensify and sharpen the supervisory action on financial sector operators who will have to be prepared for dealing with the authorities.

The new ICT risk management framework requires establishing risk tolerance levels for ICT outages, supported by performance indicators and risk metrics. Operators must also identify their "critical or important functions" (CIFs) and map their related assets and interdependencies. The inclusion of the concept of CIFs in the finalized text of DORA is a significant development that sharpens the focus of the entire framework (with particular regard to incident reporting, testing, and third-party risk management). Adherence to the requirements in this field will require most operators to broaden and strengthen their operational resilience capabilities, to define and articulate their risk appetite for disruption to critical

functions (not merely due to a technology failure or cyber incident) in a clearer manner, and to be able to map and better understand the interconnections between their ICT assets, processes, and systems and how they support service delivery.
A new element in the finalized text of the DORA is the requirement to conduct business impact analyses based on "severe business interruption" scenarios, requirement also included in the EBA guidelines. This requirement will increase supervisory pressure toward the development of more sophisticated methods of building and testing risk scenarios - a trend that is already being observed in the UK for operators required to apply the new UK operational resilience framework- and the enhancement of the redundancy and replaceability levels of systems that support CIFs.

2. ICT incident classification and reporting - consolidation of existing requirements with significant evolutionary aspects

DORA requirements regarding incident reporting will streamline a number of existing EU obligations for financial sector operators by strengthening their scope. The new requirements aim to create a new framework for classifying, notifying, and reporting incidents; this will require financial sector operators to strengthen their ability to collect, analyze, scale, and disclose information about ICT incidents and threats. In the current market environment, most operators do not have sufficient capabilities to assess the quantitative impact of incidents and analyze their root causes in line with DORA standards.

The DORA finalized text also integrates significant cyber threats as one of the case scenarios of incidents to be classified; however, in line with the changes to the Network and Information Security Directive (NIS Directive), reporting of these incidents will be optional. Conversely,in the event that a customer or counterparty is exposed to a significant cyber incident, DORA requires operators to notify and provide adequate information on protective measures. The new standards also include a requirement to record all significant cyber threats, which will require more advanced cyber incident monitoring, management and resolution capabilities.

As for reporting of ICT-related incidents, the regulation's final text removes all of the deadlines in the original proposal and delegates the responsibility for specifying them to the European supervisory authorities (EBA, ESMA, EIOPA) in the technical standards (within 18 months of the regulation's entry into force). A clearer picture of the operational impacts in this area will therefore have to wait.

Finally, a joint report is expected from the European Supervisory Authorities (ESAs) on the outcomes of the feasibility assessment regarding further centralization of the incident reporting process through the establishment of a single EU Hub for ICT incident reporting. Simplifying the reporting process would reduce the burden of fulfilling multiple reporting requirements while fostering a better understanding of cyber threats on a cross-border basis.

3. Digital operational resilience testing - new challenging requirements

DORA includes digital operational resilience level testing requirements for all entities included in the scope (except micro-entities) that include the responsibility to:

- demonstrate the conduct at least annually of an adequate set of security and resilience tests on their "critical ICT systems and applications" (a potentially more specific level than CIFs);
- address vulnerabilities identified by the tests. Coupled with the requirement on business impact analysis, this could become a significant area of scrutiny by regulators that could push operators to develop more extensive and accurate testing and scenario analysis capabilities, as compared to the models currently in use;
- in addition, entities that overcome a certain threshold of relevance and systemic maturity (which will be specified by the Regulatory Technical Standards) will be required to conduct "advanced" Threat Lead Penetration Tests (TLPTs) every three years (unless otherwise stipulated by national authorities on an individual basis).

In this regard, the regulators have specified that the methodology for TLPT testing must be developed in line with the European Central Bank's (ECB) TIBER-EU framework, so that practitioners who are already conducting or have planned to conduct such tests can leverage their investments to also meet DORA requirements.

DORA also requires the inclusion of all external vendors supporting critical or important functions (CIFs) in advanced testing exercises (TLPTs). This practice has to date been rarely implemented and will certainly require significant effort in planning as well as timely mapping of critical external suppliers. In the event that one of the vendors is unable to participate in testing for security reasons, DORA allows the vendor itself to conduct its own TLPT in the form of "pooled testing" for the industry entities for which it provides services. This, to date, is an area of "shared assurance" that has yet to be developed and will require shared collective action at the industry level in order to be implemented.

4. Third-party risk governance and management - strengthening the European framework in the financial sector

The third-party risk management requirements under DORA appear to be aligned with current ESA guidelines, also providing for a broadening of the scope of application given that current ESMA and EIOPA guidelines only cover outsourcing to critical suppliers (CSPs). DORA will therefore extend the requirements of the ICT outsourcing perimeter to non-critical providers also to operators who do not already apply the EBA guidelines.

DORA requirements for third-party risk management, in line with the ESAs guidelines, provide a set of minimum contractual conditions that operators must include in ICT outsourcing contracts by the DORA implementation deadline of Q4 2024. The provision of specific contract terms by a binding legislative provision such as DORA will increase the bargaining power of industry operators in negotiating such terms with suppliers, an aspect on which there has been no concrete evidence in the past. It is also expected that some contract terms, such as the vendor "unrestricted access to premises" clause featured in contracts supporting critical or important functions, will entail a path to implementation that is relatively less simple compared to other terms.

While constructing DORA, the regulation was amended to make the development of a "holistic multi-vendor strategy" an optional component of the overall ICT risk management strategy, although

supervision authorities will still have several leverage points to direct operators in this direction. Indeed, it is required to conduct a concentration risk assessment of all outsourcing contracts that support critical or important functions: this is an aspect that could make it difficult to justify specific decisions on operating models without the adoption of a multi-CSP or multi-vendor approach, or to demonstrate the rationales for which this approach is deemed unnecessary.

5. Framework for the supervision of critical ICT vendors - the world's first third-party supervision regime initiative in the financial sector

ESA's new supervisory powers, as provided in the original DORA proposal, were largely retained in the finalized text. This implies that providers designated as critical will be subject to broad supervisory powers that will allow the ESAs to assess them, require them to modify security measures, and sanction them for noncompliance with requirements. Providers will be pushed to demonstrate their ability to strengthen the level of operations resilience in support of financial sector players, with a particular focus on cases where the services provided impact critical or important functions.

Several protections were also added in the regulation with regard to the authorities' abilities to require operators to suspend or terminate their contracts with critical providers. Obviously, these powers will be exercised only in exceptional cases and after an evaluation of their industry-wide impact.

The final version of DORA also significantly expands the role of the Joint Oversight Forum (JOF), a group consisting of the European Supervisory Authorities (ESAs), other competent authorities, supervisors and independent experts. The JOF will play a greater role in the development of best practices for the oversight of critical providers and may eventually establish more accurate standards for the expected level of resilience of such providers.

Part II: Important technical standards are coming

A key feature of the DORA regulation is the delegation to secondary regulation (known in EU policy as "Level 2") of the technical details on the operational functioning of the new norms. The European Supervisory Authorities (ESAs) will develop the operational rules mainly as Regulatory Technical Standards (RTS) or Implementing Technical Standards (ITS). Regarding the critical supplier supervision framework, the European Commission will develop two Delegated Acts (see Table 1 for a list of all DORA Level 2 measures).

The process of regulatory Level 2 rulemaking implies an additional 12 to 18 months of regulatory uncertainty for operators with respect to some portions of the regulation, notably the ICT incident reporting framework and the rules and scope of advanced resilience testing. During this time frame, operators will still need to pursue the compliance process based on the primary regulatory text (Level 1) . Operators will also need to act proactively, rather than reactively, being careful to the versions in consultation of the RTS/ITS as they are released, being usually quite close to the final versions.

Table 1: Timeline for the development of DORA Level 2 regulation

Level 2 mandate	Deadline for final ESAs standards
RTS on ICT incident classification procedures and cyber threats	12 months from entry into force (estimated for Q3 2023)
RTS on the level of detail required in third-party provider management strategies (TPPs)	
RTS on the additional elements of the ICT risk management framework	
ITS on the Register of information relating to contractual agreements with suppliers in the ICT field	
RTS on reporting serious ICT and cyber incidents to authorities	18 months from entry into force (estimated for Q1 2024)
RTS on scope and additional elements for advanced testing	
RTS on key contractual arrangements for the subcontracting of functions/services in support of critical or important functions	
RTS on the appointment of members of a Joint Examination Team	
RTS on the information to be provided by a CTPP to supervisory authorities (so-called RTS on the information to be provided by a CTPP). Lead Overseer)	
European Commission Delegated Act on the Designation of Critical service Providers (CTPP)	
European Commission Delegated Act on Supervisory Fees for Critical service Providers (CTPP)	
ESA report on the creation of a central EU hub for incident reporting	24 months from entry into force (estimated for Q3 2024)

Part III: Time for industry practitioners to act

The finalization of DORA requires financial sector operators to start planning for the required implementation of the new and enhancedrequirements.. As mentioned in the introduction of this analysis, we strongly believe that DORA will change the way FS practitioners' approach operational

resilience, as it will challenge them to embrace a holistic view of resilience and develop new and sophisticated capabilities in areas such as: identifying critical or important functions, incident reporting, measuring business impact, and testing. DORA should be seen by practitioners as a catalyst for promoting strategic change in the way they manage digital risks and by strengthening the level of awareness with which management and boards are able to assess the business impact of operational disruptions, as well as understand the mitigation measures available to them.

Achieving what is required by the new regulatory standards in a 24-month period is a major challenge, considering also that practitioners will have to consider Level 2 technical standards as they are finalized. In this context, it is crucial for the practitioners to be focused on and prepared to address the following two issues:

1. Strong supervisory action in the ICT field: from its formal enactment, DORA will give national and European supervisory authorities new and wide-ranging powers in the field of digital operational resilience. Therefore, DORA should not be seen as a mere regulatory compliance exercise, but as an enabler for enhancing the level of operational resilience and capabilities in this area. As the level of understanding of the level of operational resilience by supervisors increases, so will the expectations and demands on practitioners, which the experience of the UK in the implementation of the new UK operational resilience supervisory framework shows. Practitioners also need to be aware that the involvement of multiple competent authorities, with often not perfectly aligned objectives and priorities, increases the complexity level of the compliance journey and interlocution.

   In order to understand how supervisory approaches will develop, practitioners should pay particular attention to those areas of DORA that require systemic outputs, which supervisors will certainly challenge. For instance, the new requirements for business impact analysis listed in the ICT risk management chapter, along with the requirement to conduct at least annual resilience testing for systems supporting critical or important functions and to address any identified vulnerabilities, are significant areas of monitoring that will undoubtedly be challenged by supervisors. Supervisors are likely to insist on the level of severity of the scenarios used, the sophistication of the testing methodologies, the granularity of the mapping of the systems underlying critical or important functions, and the thoroughness of the remediation plans against detected vulnerabilities.

2. Identification of areas that will require investment and an evolutionary path: many of the new requirements listed in the DORA will necessitate substantial investment in strengthening the governance, risk and compliance framework in ICT, Cyber and Third-Party Risk Management, as well as work plans to address operational vulnerabilities that emerge. Practitioners should conduct an impact analysis of the final DORA (Level 1) requirements, dynamically updating and expanding it as draft Level 2 (RTS/ITS) regulatory standards are released, so as to identify and assess current gaps in capabilities, resources and competencies that will need to be corrected during the 24-month compliance period. Based on our assessments of the finalized DORA text, the gap analysis should focus in particular on:

   - ICT risk governance framework, including the identification of critical or important functions (CIFs);
   - Maturity level of incident and threat data collection and analysis processes;
   - Level of maturity of testing scenarios and ability to construct high severity scenarios;

- ICT outsourcing processes and data (including the ability of practitioners to analyze risks of concentration on third and fourth parties).

Some relevant financial operators in terms of size and complexity, such as large cross-border groups, may currently have a higher level of maturity and capability than others, resulting in advantages on the path towards compliance with the new DORA requirements. However, supervisors are more likely to have higher expectations of large operators and expect market-leading capacity from operators for whom operational disruptions could have systemic consequences, given the criticality of the services provided. All operators, therefore, will inevitably be tested in the 24-month adjustment period starting at the end of this year. For this reason, it is not feasible to delay the process since it is crucial to start planning today for the compliance with the new regulatory standards.

Contacts

Andrea Rigoni
EU Digital Policy Center Director – Deloitte Risk Advisory
Tel: + 39 3355772342
arigoni@deloitte.it

Gianfranco Tessitore
Partner | Regulatory Strategy & Controls Transformation Leader – Deloitte Risk Advisory
Tel: + 39 3488862150
gtessitore@deloitte.it

Deloitte Risk Advisory S.r.l. S.B.
Via Tortona 25, Milano, 20144, Italia