Deloitte.

Regulatory News Alert

The EU's Digital Operational Resilience Act has been agreed: implications for the financial services sector

25 July 2022

At a glance:

- *A final agreement has been reached on the EU Digital Operational Resilience Act (DORA). The DORA represents the EU's most important regulatory initiative on operational resilience and cyber security in the financial services (FS) sector and goes a considerable way to consolidating and upgrading the requirements firms will face.*
- *The DORA will require firms to adopt a broader business view of resilience, with accountability clearly established at the senior management level. It applies to the vast majority of FS firms operating in the EU and establishes binding rules for ICT risk management, incident reporting, resilience testing and third-party risk management (TPRM).*
- *The DORA also establishes the world's first framework that allows FS supervisors to oversee Critical ICT Third Party Providers (CTPPs) including Cloud Service Providers (CSPs).*
- *The agreement now published gives firms a basis on which to begin work to prepare for implementation. It is expected to be finalised in the October's European Parliament plenary session.*
- *Firms should now conduct a gap analysis to develop a roadmap to design and implement an enhanced operational resilience framework by Q4 2024, in line with DORA's new requirements.*
- *Firms should also consider how the DORA can act as a catalyst for how they manage digital risks and how they understand the impact of operational disruptions on their business and customers.*
- *In this analysis, produced with Deloitte's expert colleagues around Europe, we explore the significant changes that firms will need to make as a result of DORA and potential implementation challenges across the five pillars of the DORA agreement.*

Introduction

EU negotiators have now **reached a full technical agreement on the DORA package**. A few months of administrative process are left before the DORA will be published in the EU Official Journal (OJ)[1], but the full text of the agreement has now been published by the European Parliament and FS firms need to begin assessing what it means for them. Our view is that the

[1] The DORA agreement will have to be translated into the EU's 25 official languages over the summer and a final approval vote by the European Parliament plenary session is needed before OJ publication can occur.

DORA is a "game changer" that will push FS firms to understand fully how their ICT, operational resilience, cyber and TPRM (Third Party Risk Management) practices affect the resilience of their most critical functions as well as develop entirely new operational resilience capabilities such as advanced scenario testing methods.

Firms will face a relatively tight 24-month implementation period in order to do this. The implementation period will begin 20 days after OJ publication (October-November this year). That means that, **by Q4 2024, relevant FS supervisors will expect firms to be in full compliance with all of the DORA's new requirements**, including how those requirements are elaborated through secondary rulemaking by the European Supervisory Authorities (ESAs) (see Part II below).

Part I: What does the final DORA agreement mean for firms? – analysis across the DORA's five pillars

The version of the DORA that has been agreed by legislators preserves the five key pillars of the original proposal from the European Commission. From our analysis of the final technical agreement, we see the following implications:

1. ICT risk management requirements – a broader focus across critical business functions

The DORA's ICT risk management framework puts the onus on the firm's management body to take "full and ultimate accountability" for the management of ICT risks, for setting and approving its digital operational resilience strategy, and for reviewing and approving the firm's policy on the use of ICT Third Party Providers (TPPs), among other responsibilities. The DORA gives competent authorities the power to apply administrative penalties and remedial measures on members of the management body for any breaches of the Regulation.

The DORA's ICT risk management requirements are largely in line with the Guidelines from the EBA on ICT Security and Risk Management (2019) and from EIOPA on ICT Security and Governance (2020), but their newly binding nature through now being in primary legislation will intensify the supervisory scrutiny that firms can expect to face.

The **ICT risk management framework requires firms to set risk tolerances for ICT disruptions supported by key performance indicators and risk metrics**. Firms must also **identify their "Critical or Important Functions"** (CIFs) and map their assets and dependencies. The inclusion of CIFs in the final DORA text is a significant evolution and refines the focus of activity throughout the entire framework (particularly re: incident reporting, testing and TPRM). Meeting these requirements will challenge most firms to broaden their operational resilience capabilities, more clearly articulate their risk appetite for disruption across critical functions (not just for technology failure or a cyber incident), and more accurately be able to map and understand the interconnections between their ICT assets, processes, and systems and how they support service delivery.

A new inclusion in the final DORA text is the requirement for firms to carry out business impact analyses based on "severe business disruption" scenarios (also present in the EBA Guidelines). This will likely contribute to growing supervisory pressure for firms to develop more sophisticated scenario testing and to build redundancy and substitutability into the systems that support their CIFs.

2. ICT incident classification and reporting – consolidation of existing requirements but with significant enhancements

The DORA's incident reporting framework is meant to streamline a number of existing EU incident reporting obligations that apply to FS firms. It will nevertheless create a substantial new classification, notification and reporting framework that will challenge firms to improve

their ability to collect, analyse, escalate, and disseminate information concerning ICT incidents and threats. In our view, **most firms do not currently possess all the capabilities needed to assess the quantitative impact of incidents** and analyse their root causes in the way they will need to under the DORA.

The final DORA text adds "significant cyber threats" to the list of events that firms must classify, but in line with parallel amendments made to the Network Information Security Directive (NIS2) reporting them will be optional. However, in the event that a client or counterparty is exposed to a significant cyber threat, the DORA requires FS firms to notify them and to provide information on appropriate protection measures to defend against the threat. Entities are also required to record all significant cyber threats, which will require a higher incident management capability to monitor, handle and resolve cyber incidents.

For the ICT-related incident reporting, the **final text deletes all the original reporting deadlines** of the proposal and delegates this **to the ESAs to specify in technical standards** (due 18 months after entry-into-force). For firms, this means that a clearer view of the operational feasibility of the new framework will not come for some time.

Finally, the ESAs are also expected to prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by firms. Streamlining ICT-incident reporting is expected to reduce the burden of complying with multiple incident reporting requirements in the financial sector, while also supporting a better collective understanding of cyber threats on a cross-border basis.

3. Digital operational resilience testing – introducing challenging new requirements

The DORA establishes a digital operational resilience testing requirement for all in-scope firms (except for microenterprises) where they will have to:

- show that they conduct an appropriate set of security and resilience tests on their "critical ICT systems and applications" (a potentially more granular definition that CIFs) at least annually;
- "fully address" any vulnerabilities identified by the testing. Together with the business impact analysis requirement, this could evolve into a significant area of supervisory scrutiny and push firms to develop broader and more accurate testing and scenario analysis capabilities; and,
- firms above a certain threshold of systemic importance and maturity (to be specified by a Regulatory Technical Standard (RTS)), will need to conduct "advanced" Threat-Led Penetration Testing (TLPT) every three years (unless amended by national authorities on a firm-by-firm basis).

Negotiators chose to specify that the methodology for the TLPT testing should be developed in line with the ECB's existing TIBER-EU framework, so firms currently running or moving towards TIBER testing can have some confidence that this work will count towards the DORA's advanced testing requirements.

The DORA also requires FS firms to include all TPPs supporting CIFs in advanced testing exercises. This is rarely done in TLPT exercises in the FS sector today, and something that will likely require significant planning and mapping of TPPs to CIFs. If a TPP cannot participate for security reasons, the DORA allows for the TPP to conduct its own TLPT as a form of "pooled testing" for the FS firms to which it provides services. This is a developing area of shared assurance, but one which will need collective action from the FS industry to operationalise.

4. TPRM – strengthening the European FS framework

The TPRM requirements in the DORA are broadly aligned to the existing ESAs' Guidelines, but ESMA and EIOPA's Guidelines only cover outsourcing to CSPs. The DORA will therefore expand these requirements to non-CSP ICT outsourcing for firms not applying the EBA Guidelines.

The DORA TPRM requirements, like the ESA Guidelines, contain a number of contractual terms that firms must include in ICT outsourcing contracts by the implementation deadline in Q4 2024. Placing these in binding law, as the DORA does, will increase the pressure on FS firms to negotiate these terms with their providers where they have been unsuccessful before. Certain terms, such as the TPP providing "unrestricted access to premises" in contracts supporting CIFs, may be more difficult to implement than others.

The DORA was amended in negotiations to make the development of a "holistic multi-vendor strategy" an optional part of the ICT risk management strategy, but supervisors will still have several levers to use to influence firms here. Firms must conduct concentration risk assessments of all outsourcing contracts that support the delivery of CIFs. This will be a challenging task in itself, but also one which may make certain operating model decisions difficult to justify to supervisors without the adoption of a multi-CSP or multi-vendor approach or having a credible resilience framework to demonstrate why this is not needed.

5. CTPP oversight framework – the world's first FS oversight regime for third parties

The new oversight powers of the ESAs from the original DORA proposal are largely maintained by the final agreement. This means that TPPs that are designated as "critical"[2] will be subject to extensive supervisory powers that will allow the ESAs to assess them, ask them to change security practices, and sanction them if they do not. This will push CTPPs to demonstrate that they can improve the resilience of their own operations that support FS firms, and particularly where the CIFs of FS firms are implicated.

Several new safeguards have been added into the final DORA text around the ability of authorities to order FS firms to suspend or terminate their contracts with CTPPs. This should provide firms with some added confidence that these powers will only be used in exceptional circumstances and with due regard to the impact they would have on the sector.

The final version of the DORA also significantly expands the role of the Joint Oversight Forum (JOF), a group of the ESAs, relevant authorities, supervisors, and independent experts. **The JOF will now play a more important role in developing consistent best practices for the oversight of CTPPs, and could, over time, establish a clearer standard for their expected level of resilience.**

Part II: Important technical standards are still coming

A key feature of the DORA agreement is the extent to which critical details about how the new rules will function in practice are delegated to secondary rulemaking (known in EU policy as "Level 2"). In most cases, the ESAs working together in the Joint Forum will develop these rules as RTS or Implementing Technical Standards (ITS). In the case of the CTPP oversight framework, the European Commission will develop two Delegated Acts (see Table 1 below for a list of all Level 2 measures in the DORA).

One practical implication of the Level 2 policy process is that there will be another 12–18-month period of policy uncertainty for firms in some areas of the Regulation, particularly regarding the ICT incident reporting framework and the rules and scope for advanced resilience testing, among others. During this time, firms will need to forge ahead with implementation work that they can initiate based off the Level 1 text. Firms should also pay close attention to

[2] The precise criteria and procedures for designating a TPP as "critical" will be set out in a Delegated Act that the European Commission will develop and finalise by 18 months after the DORA's entry-into-force.

the consultative versions of the RTSs/ITSs when they are released, as they usually are quite similar to the final versions that are eventually adopted by the ESAs.

Table 1: The DORA's Level 2 mandates and timing

Level 2 mandate	Deadline for final ESAs standard
RTS on ICT incident and cyber threat classification procedures	12 months after entry-into-force (Estimated for Q3 2023)
RTS on level of detail required in firms' ICT TPP strategies	
RTS specifying further elements of the ICT risk management framework	
ITS on the Register of Information on ICT third party contractual arrangements	
RTS on reporting of major ICT and cyber incidents to authorities	18 months after entry-into-force (Estimated for Q1 2024)
RTS on scope and additional elements for advanced testing requirements	
RTS on key contractual provisions for subcontracting functions that support CIFs	
RTS on the designation of members of a Joint Examination Team	
RTS on information to be provided by a CTPP to the Lead Overseer	
Delegated Act from the Commission on CTPP designation	
Delegated Act from the Commission on oversight fees for CTPPs	
ESA report on the establishment of a central EU-hub for incident reporting	24 months after entry-into-force (Estimated for Q3 2024)

Part III: Now is the time for firms to act

Now that the technical agreement on the DORA has been finalised, FS firms need to begin to plan seriously for the task of implementing the Regulation. As we have said earlier in this analysis, **we believe the DORA to be a game changer for how every FS firms approach operational resilience**, as it will push them to take a broader view of resilience and develop sophisticated new capabilities in areas such as CIF identification, reporting, impact measurement and testing. The DORA should be seen as a catalyst for firms to accelerate strategic change in how they manage digital risks, and how effectively senior management and boards are able to evaluate the business impact of operational disruptions and understand the mitigants at their disposal.

Doing all of this in a 24-month period will be a significant task, not least as firms will have to factor in Level 2 technical standards as they become available and are finalised. Getting a head start before the implementation period begins later this year will buy firms valuable time to prepare. In particular, firms should bear the following two considerations in mind:

1. **Prepare for increased supervisory engagement**: when the DORA enters into force, it will grant national and EU-level supervisors sweeping new mandates and powers on digital operational resilience. Instead of seeing the DORA as a "box ticking" compliance exercise, firms should expect their relevant authorities to develop supervisory frameworks that use their new powers to push firms to improve their ability to assess

and enhance their operational resilience-related capabilities. As supervisors' own understanding of operational resilience increases, so too will their likely demands for firms. Firms should also be conscious that where multiple authorities are involved, whether prudential/conduct, home/host, or national/EU-level, differing supervisory objectives and priorities around the impact of ICT disruptions may make keeping up with expectations even more challenging.

To understand how these supervisory frameworks are likely to develop, firms should focus on areas of the DORA that demand regular outputs that can be challenged by supervisors. For instance, the new business impact analysis requirements in the ICT Risk Management chapter, read alongside the requirement for firms to carry out resilience testing for systems supporting CIFs at least annually and to "fully address" any vulnerabilities identified look set to amount to a significant area of scrutiny for firms. Supervisors are likely to push them here on the severity of scenarios used, the sophistication of testing methods, the granularity of the underlying systems mapping and the completeness of remediation work to address vulnerabilities.

2. **Identify capabilities that will require investment/development**: many of the DORA's new requirements will demand substantial investment in the governance, risk, and compliance framework around ICT, Cyber and TPRM functions as well as follow-on work to address operational vulnerabilities that are identified. Firms should conduct a gap analysis based on the final requirements in the DORA Level 1 text, updating it as draft Level 2 standards become available, to identify where capability, resource and expertise shortfalls currently exist and will need to be corrected during the 24-month implementation period. Based on our analysis of the final DORA agreement, this gap analysis should focus in particular on:

- ICT risk governance practices including the identification of CIFs;
- The maturity of incident and threat data collection and analysis capabilities;
- The sophistication of scenario testing and severe scenario design (as discussed in the point above); and
- The integration of ICT outsourcing processes and data (including the ability of firms to analyse concentration risks in third and fourth parties).

Some parts of the FS sector, such as large cross-border groups, will have higher levels of current-state capabilities than others and may have a head start in complying with the DORA's new requirements. Supervisors, however, are likely to expect better-developed capabilities from larger firms, and market-leading capabilities in firms where operational disruptions could have systemic consequences due to the criticality of their services. All firms are, therefore, likely to be challenged by the DORA and the 24-month implementation period that will begin later this year. They should waste no time and begin to plan for the DORA's implementation today.

How Deloitte can help

Deloitte can help you along the entire journey towards compliance with DORA by assessing your current readiness and proposing measures to meet the regulatory requirements while customizing the remediation plan to your specific environment. Deloitte can help with different activities allowing you to improve your current capabilities and to implement DORA's new requirements.

Deloitte.

Deloitte can also help you to stay on top of the regulatory agenda with its regulatory watch service and keep you up to date on the evolution of DORA and other regulations.

Deloitte.

Your Contacts

Subject matter specialists

Irina Hedea
Partner – Information & Technology Risk
Tel: +352 45145 2944
ighedea@deloitte.lu

Maxime Verac
Director – Information & Technology Risk
Tel: +352 45145 4258
mverac@deloitte.lu

Yasser Aboukir
Director - Cyber Risk Services
Tel: +352 451 452 299
yaboukir@deloitte.lu

Stephane Hurtaud
Partner – Cyber Security Leader
Tel: +352 45145 4434
shurtaud@deloitte.lu

Laureline Senequier
Director – Risk Advisory
Tel: +352 45145 4422
lsenequier@deloitte.lu

Aleksandra Suwula
Manager – Risk Advisory
Tel: +352 45145 3718
asuwala@deloitte.lu

Regulatory Watch Kaleidoscope service

Jean-Philippe Peters
Partner – Risk Advisory
Tel: +352 45145 2276
jppeters@deloitte.lu

Simon Ramos
Partner – IM Advisory & Consulting
Tel: +352 45145 2702
siramos@deloitte.lu

Marijana Vuksic
Senior Manager – Risk Advisory Tel:
+352 45145 2311
mvuksic@deloitte.lu

Benoit Sauvage
Director – Risk Advisory
Tel: +352 45145 4220
bsauvage@deloitte.lu

Deloitte Luxembourg
20 Boulevard de Kockelscheuer
L-1821 Luxembourg
Grand Duchy of Luxembourg

Tel: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu