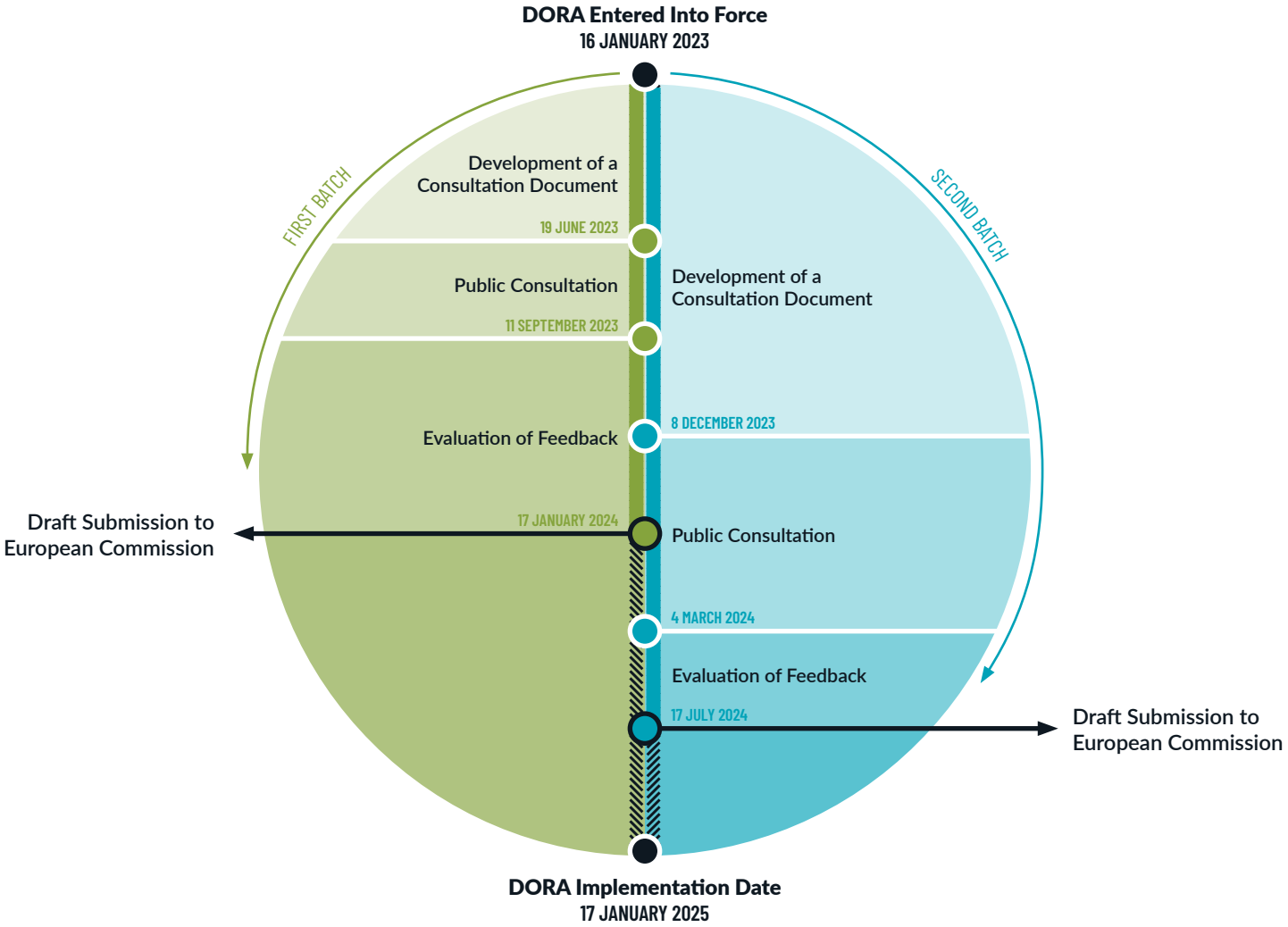
DORA Compliance: Untangling Key Hurdles to Implementation

Table of Contents

Introduction

The Digital Operational Resilience Act (DORA), or more formally known as Regulation (EU) 2022/2554, took effect on 16 January 2023, with final industry compliance required by 17 January 2025. The regulation underscores the importance of digital operational resilience in today's increasingly interconnected and digitised landscape and seeks to expand the reach of European regulators incorporating both financial institutions that operate in Europe and providers of information and communication technology (ICT) to these firms. Compliance with DORA is a top priority given financial entities' dependence on ICT, including third-party ICT service providers, as well as the heightened focus on ICT and cyber-related risks impacting these third parties.

Understanding the full implications of the DORA text and aligning with its intent have been challenging for many financial institutions despite being more than a year into implementation. Finalised standards are expected on 17 July 2024, providing firms with six months to analyse the text amendments, assess feasibility of available options, and implement the requirements. Following this, it may take additional months before the European Commission publishes the final Delegated Regulations,[1] as was the case with the first batch of Technical Standards. Firms will likely choose not to wait for the release of the Commission Delegated Regulations to begin compliance, hence firms will face a degree of uncertainty until they are published.



1. The European Commission has adopted three more Delegated Regulations for DORA and is now for European Parliament and the Council of the EU to scrutinise and adopt the delegated acts. Refer to: https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en.

Key Industry Challenges

With the deadline for compliance rapidly approaching, there are some concerns with firms' abilities to respond to and apply the DORA requirements by the implementation date, particularly for firms that had not already built most of the required capabilities. Five key concerns are presented below.

DORA Entered Into Force
16 JANUARY 2023

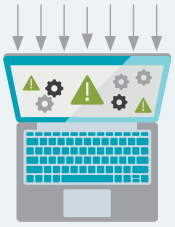
1

Constraints with obtaining data points and conducting analysis may lead to excessive reporting, detracting from the effective management of ICT-related incidents.

2

The large volume of potentially in-scope ICT third-party providers, lack of automation and extensive amount of information pose challenges and, in some cases, complexities fulfilling the third-party risk management requirements, including contract management and completion of the register of information.

3

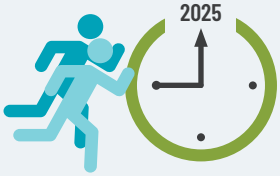


The potentially broad scope of threat-led penetration testing (TLPT) and the involvement of third-party providers in the scope of a firm's TLPT could place pressure on firms' ability to manage the TLPT exercise.

4

The broad nature of DORA definitions and questions concerning the notion of proportionality result in an overly expansive scope, which could lead to extensive time and effort required to comply.

5



The January 2025 compliance date may be impractical for some firms without a proportionate approach to supervision and enforcement.

DORA Implementation Date
17 JANUARY 2025

1. Constraints with obtaining data points and conducting analysis may lead to excessive reporting, detracting from the effective management of ICT-related incidents.

The final technical standard for ICT-related incident classification has been released, and along with the additional draft requirements for compulsory and standardised incident reporting further raises concerns that a strict interpretation could result in a disproportionate amount of reporting at the expense of effectively managing ICT related incidents.

- The potential for over-reporting could dilute the effect of truly meaningful notifications. This may also contribute to a material increase in overhead associated with all incidents.
- The definition of 'critical services affected' within the Delegated Act on classification of major incidents is lacking in proportionality and is at risk of capturing essentially all incidents, by virtue of Article 6(b), which references the impact of any service which requires authorisation, registration, or that is supervised. Firms may struggle to create the data-collection tools and processes needed to fully comply with this requirement, leading to excessive time and effort needed for data collection over incident management.
- Clarification is sought in terms of the intent of criteria detail in Article 6(b) (i.e., 'affects financial services that require authorisation registration or are otherwise supervised by competent authorities'). AFME has called on the European Supervisory Authorities (ESAs) to require all three classification criteria to be met, as opposed to 'any' or a single criterion. Some believe the current draft should be interpreted to require firms to report on every major ICT-related incident, or security or operational payment-related incident, given the expansive purview of the criteria. As a result, some firms are interpreting the draft to require that an incident be assumed notifiable until evidence can be obtained to demonstrate that it is not major, creating significant overreporting.
- If the root cause of an ICT-related incident is the same as any major or non-major ICT-related incident in the previous six months, then both incidents would need to be reported. In addition, the requirement to report recurring incidents will make it necessary for firms to conduct a root cause analysis on all ICT-related incidents, no matter the severity. It represents a material reallocation of incident management resources toward documentation and classification work. In practice, given the unfeasibility of conducting this analysis across all ICT-related incidents, firms will need to apply their own internal classification to determine which ICT-related incidents to assess according to the DORA requirements.
- The attribution and subsequent tagging of incidents is typically conducted at the enterprise level given most firms are running global systems, rather than at the legal entity level. Understanding the change impact, related dependencies, third-party relationships, and ultimate jurisdictional impact at a legal-entity level is predicted to be a significant challenge for firms.

Significant amount of time and resources will likely be needed for firms to meet the incident reporting requirements by the January 2025 implementation date; in addition, the significant incremental amount of time and resources would persist into perpetuity.

2. The large volume of potentially in-scope ICT third-party providers and the lack of automation poses complexities with fulfilling the third-party risk management requirements, including contract management and completion of the register of information.

Third-party risk management and subsequent contract management raises concerns across the sector given the material number of third-party providers and subcontractors within firms' service supply chains.

- The task of filling out numerous fields in the Register of Information, particularly across diverse populations of ICT third-party service providers and subcontractors, is daunting. The register requires several new data points previously not required for EU outsourcing registers by financial entities. It may also require certain subcontractors to be treated as direct third-party providers for the purposes of the Register, despite the lack of direct contractual agreement.[2] Given that the primary objective of the DORA register is to provide authorities with insights into critical third-party providers and to help inform their designation under the DORA oversight framework, there is a shared sentiment across institutions that this task may not be in proportion to its intended purpose. Leniency on the delivery dates for certain data requirements would be welcomed, for example on providing Legal Entity Identifiers (LEIs) for all ICT third-party providers.
- Authorities continue to overestimate the extent of automation of data-collection processes; many firms will be dependent on manual efforts to maintain and submit the register of information. There is minimal confidence in existing repositories that are comprehensive, current, and in the prescribed format required by DORA, thus requiring substantial reliance on the broad network of relationship owners and service subject matter experts to obtain or reformat this data. Consequently, this could lead to a high degree of discrepancy in the quality and accuracy of the data.
- The time frames to review and renegotiate the volume of contracts by January 2025 may not be feasible without a proportionate approach to supervision by the authorities. Further, there is no assurance that vendors will be willing to accept the contractual changes. Requiring financial entities to oversee the entire subcontracting chain of their ICT providers and to review contracts between their vendors and their subcontractors is a challenge and subject to commercial sensitivities. This may create confusion by obligating the financial entity to act like a supervisor, which is not the intent of the regulation.

AFME has called for the ESAs to explicitly set out in the final report due 17 July 2024 that it is limited to those sub-contractual arrangements effectively underpinning *Critical or Important Functions* (CIFs), as was the case with the Delegated Act for the Register of Information.

3. The potentially broad scope of threat-led penetration testing (TLPT) and the involvement of third-party providers in the scope of a firm's TLPT could place pressure on firms' ability to manage the TLPT exercise.

The limited experience and minimal level of guidance to execute threat-led penetration testing (TLPT) alongside third parties may constitute a risk to financial institutions. Further consultation with the industry is sought before pooled testing and the inclusion of third-party providers can be considered feasible. There is also ambiguity in the RTS[3] concerning the application of TLPT to Critical or Important Functions (CIFs). This could drive excessive testing if TLPT becomes a 'tick-box' exercise requiring evidence against every CIF.

2. The Final Report on Draft Regulatory Technical Standards specifies the criteria for the classification of ICT-related incidents, materiality thresholds for major incidents and significant cyber threats.
3. The RTS will specify threat-led penetration-testing aspects.

- The RTS on TLPT has unclear language regarding how a TLPT authority would consider the scope or relevance of a test for *'the facilitation of mutual recognition'*. The reference to CIFs within the Technical Standard's text and supporting Annex infers that a TLPT could be on the basis of services, instead of the defensive capabilities of financial entities. Additionally, for the purposes of management reporting, there are concerns whether the testing would be duplicative, in terms of the infrastructure and underlying assets and systems. While CIFs may be an appropriate targeting mechanism, attempting to cover all CIFs, or to view TLPT as a standard control, may introduce excessive testing across all Member States on the same ICT systems and control teams.
- The expectations for third-party involvement in TLPT activities must be clearly stipulated given the minimal level of guidance and limited experience in the sector. The authorities abstaining firms from including third parties within the scope of initial TLPT exercises, until full guidance can be developed in collaboration with industry, would be welcomed. In the absence of such clarity, a pooled test could result in significant cybersecurity risk, operational difficulty, and legal complications. AFME has called on the ESAs to develop guidance on TLPT, similar to the information provided for purple teaming exercises.

The industry welcomes the close adherence to TIBER-EU that the authorities have achieved in the draft RTS. However, the potential expansion of TLPT testing to a wide set of a firm's CIFs and the inclusion of third parties in testing may create risks to the smooth functioning of a TLPT testing programme.

4. The subjective nature of the DORA definitions and the unclear notion of proportionality may increase the scope and subsequent time and effort required to adhere to regulatory requirements.

The subjective nature of DORA definitions and terminologies, such as CIF, will influence the scope and the requisite time and effort to adhere to regulatory requirements. Firms should be proportionate by applying the compliance requirements according to their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. The concern is that firms will be reprimanded given differences in the application of proportionality across the sector or on the basis of Member State supervisory perspectives.

- Firms have applied varied approaches to ensure that their CIF listing is complete and accurate, commonly weighing whether to leverage existing firmwide assessments versus regional criticality assessments of services, such as the Basel Committee on Banking Standards forums on critical operations, or the UK's important business services (IBS) methodology. An inflated final list of CIFs may have downstream implications, including additional systems falling into the purview of testing or additional service providers requiring contract renewal. This could make it hard for firms to manage their resilience programme and may create resource constraints for enhanced resilience programmes.
- The notion of proportionality appears throughout the DORA text and supporting technical standards. However, in the absence of standardised directives, there may be disparate approaches in the application of proportionality across firms. Additional prescriptive text on proportionality is not sought after. Instead, there is a desire that any differences in the interpretation and application of proportionality across the sector will not be negatively marked.

Firms are of the understanding that providing adequate rationale and holding a defensible position in their approach to CIF identification and their application of proportionality across the requirements, is sufficient in meeting the overarching regulatory mandate.

5. The January 2025 compliance date may be impractical for some firms without a proportionate approach to supervision and enforcement.

There is still ambiguity in terms of what is fundamentally required by the January 2025 compliance date and whether there is flexibility for certain requirements to be managed following this specific date.

- Taking the register of information as an example, firms may struggle to produce the requisite data from their entire supply chain if the authorities anticipate information collection by the deadline date.
- Similarly, DORA does not allow for a transitional period for contract uplift, as is standard in regulations mandating new contractual terms. Many firms will churn through numerous contracts but will only be able to commence the process of remediation when the final technical standard[4] on subcontracting is published, despite this likely being only a couple of months ahead of the January application deadline. There is also concern that needing to choose between achieving the desired contractual terms and meeting the tight deadline may lead many to accept inferior terms from their service providers.

Firms will likely have to prioritise register compilation and contract uplifts for ICT third-party service providers supporting CIFs in the first instance, and subsequently work through their contact backlog in line with contract renewals, in order to meet the January 2025 deadline.

Conclusion

The financial sector is committed to aligning with the objectives and regulatory intent of DORA. This commitment extends beyond mere compliance; it represents dedication to fortifying operational resilience for the betterment of financial institutions and to best serve customers, clients and stakeholders. Financial entities are united in working with regulatory bodies to achieve full compliance. Without untangling the complexities and challenges associated with achieving compliance, an operationally resilient and unified digital landscape becomes even more difficult to achieve.

4. The RTS will specify elements when subcontracting critical or important functions.

The Association for Financial Markets in Europe (AFME) is the voice of Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. We represent the leading global and European banks and other significant capital market players. AFME's members are the lead underwriters of 89% of European corporate and sovereign debt, and 79% of European listed equity capital issuances.

We advocate for deep, integrated, and sustainable capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

AFME works to promote a robust, connected and competitive financial system in the EU, UK and globally.

afme.eu

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Through our network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned Member Firms provide clients with consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit.

Named to the 2024 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti.com

Contacts

Marcus Corry
Director, Technology & Operations, **AFME**
marcus.corry@afme.eu

Douglas Wilbert
Managing Director, Protiviti
douglas.wilbert@protiviti.com

Laura Moore
Managing Director, Protiviti
laura.moore@protiviti.co.uk