Opening pan-DORA's box: Navigating the practical challenges of the EU's Digital Operational Resilience Act

Received (in revised form): 28th January, 2026

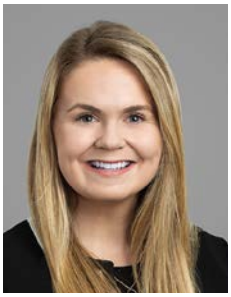
Nathaniel Lalone*
Partner, Financial Markets and Funds, Katten Muchin Rosenman UK, UK

Ciara Watson**
Associate, Financial Markets and Funds, Katten Muchin Rosenman UK, UK

Nathaniel Lalone *is a dual-qualified lawyer (England, New York) and a leader in the field of providing cross-border regulatory and compliance advice to market infrastructures as well as sell-side and buy-side firms active in the over-the-counter derivatives, futures and securities markets. Nate is sought out by clients for his ability to manage their legal and regulatory risks while helping them achieve their commercial goals. Since the financial crisis, regulation of financial markets and products has increased considerably, which has challenged existing market structures while prompting a wave of innovations and new ways of thinking. Incumbents and disruptors both compete to bring groundbreaking solutions to market while contending with overlapping, and sometimes contradictory, legal and compliance obligations. Drawing on his vast cross-border experience and deep understanding of both US and UK/EU law and regulation, Nate is able to distil complexity into clear, commercially sensible solutions to cutting-edge and often first-of-their-kind questions.*

Ciara Watson *focuses her practice on financial markets and funds. She has previous experience working in large financial institutions and uses the knowledge and expertise gained to deliver commercially focused advice to clients. Ciara works with a range of market participants who grapple with regulatory and compliance matters across the financial services sector. She advises clients on a broad spectrum of matters from reviewing and negotiating trading documentation to updating policies and procedures and providing regulatory insights and recommendations. Prior to joining Katten Muchin Rosenman UK LLP, Ciara worked in New York in the Markets Legal Department of a swap dealer. She also worked in the Regulatory Transformation team of a global investment institution. As a result, she understands and appreciates the complex regulatory issues that firms face in the financial services sector.*

Nathaniel Lalone



Ciara Watson

Abstract

The Digital Operational Resilience Act (DORA) establishes comprehensive information and communication technology (ICT) risk management requirements for EU financial entities, applying from 17th January, 2025. It mandates new frameworks for operational resilience testing, third party risk management and incident reporting, while requiring extensive provisions to be embedded in contractual arrangements with ICT third party service providers. Implementation challenges include regulatory delays, complex register of information requirements and difficult contract negotiations. To navigate DORA's complexities, financial entities should establish cross-functional governance, prioritise contract remediation by criticality and implement proportionate compliance approaches tailored to their specific risk profiles and operational circumstances. This article is also included in ***The Business & Management Collection*** *which can be accessed at https://hstalks.com/business/.*

Keywords: Digital Operational Resilience Act, DORA, operational resilience, third

Journal of Financial Compliance
Vol. 9, No. 4 2026, pp. 369–379

2398-8061 (2026)

Journal of Financial Compliance is included in **The Business & Management Collection**

party service providers, information and communication technology, ICT, risk management, contract remediation, register of information, threat-led penetration testing, TLPT, EU financial regulation

DOI: 10.69554/ATNS1453

INTRODUCTION

The EU Digital Operational Resilience Act (DORA)[1] establishes a harmonised and comprehensive digital operational resilience framework across the EU financial sector by requiring a wide range of financial entities to manage their information and communication technology (ICT)-related risks in a robust and effective manner. Although DORA has applied since 17th January, 2025, the practical implementation of this ambitious regulatory framework has revealed significant gaps between regulatory intent and operational reality. This paper examines the key challenges firms have encountered in their DORA compliance journey and explores some of the practical solutions that have emerged from implementation to date.

THE REGULATORY IMPERATIVE: WHY DORA MATTERS NOW

The digital transformation of financial services

The financial sector has become increasingly dependent on ICT and information in a digital form. The COVID-19 pandemic further exacerbated this situation, with financial institutions relying even more on the availability of digital systems to conduct day-to-day operations in remote or hybrid environments. This digital transformation has fundamentally altered and, in many ways, heightened the risk landscape for financial institutions.

Recent events have demonstrated the importance of managing digital resilience risks. For example, the July 2024 global outage triggered by a faulty CrowdStrike software update caused over 8 million computers to crash and led to widespread disruption across industries and sectors. While the error was identified and a fix was released within hours — and the financial services sector recovered relatively quickly — many other systems and economic sectors experienced prolonged outages.

In 2025, several large cloud providers experienced global-scale outages alongside smaller regional incidents. In June 2025, for instance, a software bug in Google Cloud Platform's Service Control system caused a global authentication failure, locking users out of various services and causing extensive disruption to organisations relying on Google Cloud for authorisation services. A few months later, in October 2025, Amazon Web Services experienced an infrastructure failure that triggered a multihour domino effect affecting financial and consumer platforms. Shortly thereafter, Microsoft Azure suffered an incident caused by a faulty, inadvertent configuration change in Azure Front Door, which led to node failures and widespread disruption.

Such events underscore the systemic concentration risk for financial entities within the scope of DORA. These incidents translate abstract obligations into operational challenges, reinforcing the importance of resilience requirements such as service provider tiering, rapid incident classification, evidence logging and tested exit plans under DORA.

Addressing regulatory fragmentation

Historically, there has been a lack of harmonised European rules on digital operational resilience. European Union (EU) Member States adopted national regulatory initiatives and supervisory approaches that were not perfectly aligned. Given the cross-border nature of ICT risks, action at the Member

Katten Muchin Rosenman UK LLP,
Paternoster House,
65 St Paul's Churchyard,
London EC4M 8AB,
UK

**Tel: +44 20 7776 7629;*
E-mail: nathaniel.lalone@katten.co.uk

***Tel: +44 (0) 20 7770 5231;*
E-mail: ciara.watson@katten.co.uk

State level had only a limited effect and often complicated compliance efforts where a single financial entity operated across multiple Member States. The lack of co-ordinated national initiatives resulted in inconsistencies, duplicative requirements and high compliance costs, while certain ICT risks remained undetected and unaddressed.

Prior to DORA, the EU framework was characterised by a sector-specific and piecemeal regulatory approach to operational resilience. Financial subsectors, such as banking, insurance and asset management, were subject to divergent standards and supervisory expectations, with operational resilience requirements frequently embedded in guidelines rather than binding legislation. For example, while the European Banking Authority (EBA) guidelines on outsourcing arrangements[2,3] provided important direction for banks, certain investment firms and payment institutions, the European Insurance and Occupational Pensions Authority Guidelines on ICT security and governance provided information for insurance and pension undertakings.[4] These various sectoral-level guidelines did not apply uniformly across the financial sector. This fragmented approach created further regulatory uncertainty, inconsistent implementation and gaps in oversight, particularly in the context of cross-sector and cross-border ICT dependencies.

DORA replaces this patchwork of national regulations and EU-level guidelines with a single, overarching regulation that has direct effect across all EU Member States. In doing so, it codifies aspects of existing guidelines, such as the EBA guidelines on outsourcing arrangements, and streamlines the existing patchwork of relevant provisions contained within EU financial services legislation. In addition, as an EU regulation, the provisions of DORA have direct effect in all EU Member States without requiring any national implementation measures. DORA is part of a broader framework that includes an Amending Directive,[5] which modifies existing sectoral financial directives to ensure consistency between DORA's requirements and existing financial laws. As a result, DORA and the Amending Directive together establish a single, harmonised EU rulebook governing operational resilience and ICT-related risk for all financial entities.

Comparative global perspective

Although DORA is sector-specific to financial services, its objectives — resilience, incident transparency and third party risk control — resonate across broader regulatory initiatives. Across jurisdictions and economic sectors, resilience expectations are converging around governance, testing, incident reporting and supply-chain assurance, highlighting the widespread importance of resilience and risk management.

For example, the EU's Network and Information Security (NIS2) Directive[6] harmonises cybersecurity and operational resilience obligations for entities operating in 18 sectors across the EU, including energy, transport, health and digital infrastructure, thereby establishing a cross-economy baseline. While both NIS2 and DORA emphasise supply-chain exposure, NIS2 highlights supply-chain security, whereas DORA tailors third party risk management to the specific dependencies of the financial sector. Sanctioning approaches also diverge with NIS2 specifying substantial quantified administrative fines, while DORA leaves the determination of sanctions to Member States and their national competent authorities. Where both frameworks apply to a financial entity, the *lex specialis* principle means that DORA, as the sector-specific regime, takes precedence over NIS2.

Across the Atlantic, the US Securities and Exchange Commission (SEC) has adopted rules requiring public companies subject to the Securities Exchange Act of 1934 to

enhance and standardise disclosures relating to cybersecurity risk management, strategy, governance and incidents.[7] The rules mandate disclosure of material cybersecurity incidents, as well as periodic disclosure of a registrant's processes for assessing, identifying and managing material cybersecurity risks, management's role in addressing those risks and board oversight. While the SEC regime is centred on investor transparency and materiality-driven reporting, including annual cybersecurity risk disclosures, DORA is centred on operational impact. It applies defined criteria and materiality thresholds to classify major incidents and requires firms to detect, report and remediate ICT-related risks in near real time. For international financial services firms, co-ordinated incident response and governance are therefore essential to align SEC disclosure timelines and materiality thresholds with DORA's incident classification, notification and remediation obligations.

SCOPE AND APPLICATION: UNDERSTANDING WHO IS AFFECTED

Direct application to financial entities

DORA applies to 'financial entities', a term defined broadly to cover the majority of EU financial services firms. The term applies not only to 'traditional' financial institutions (eg banks, investment firms and insurance companies), but also to 'new players' in the market, such as crypto-asset service companies and certain ICT service providers (eg cloud service providers).

Because DORA's scope extends beyond traditional boundaries, it creates complexity for non-EU entities. For example, the circumstances in which DORA may apply to third country financial entities, such as non-EU fund managers, are not entirely straightforward. DORA provides that 'managers of alternative investment funds' are 'financial entities'.[8] Read broadly, this language could encompass *any* manager of *any* alternative investment fund that is marketed in the EU. This broad interpretation has resulted in uncertainty for international firms operating in EU markets.

Critical ICT third party service providers

DORA applies to 'critical' ICT third party service providers (CTPPs). An ICT third party service provider may be designated as critical in two ways: (a) by designation from the European Supervisory Authorities (ESAs); or (b) by volunteering for designation. Such CTPPs are subject to enhanced regulatory and compliance obligations as well as direct oversight by EU authorities, including the requirements to establish an EU presence.

In November 2025, the ESAs published the list of designated CTPPs subject to direct oversight under DORA. The designation process followed the prescriptive methodology mandated by DORA and marked a significant step in implementing the DORA oversight framework. The current list includes major cloud providers, data centre operators, infrastructure and network providers and providers of financial services-specific technology. The ESAs will update and publish the CTPP list annually.

Indirect impact on noncritical ICT third party service providers

DORA also applies, albeit indirectly, to ICT third party service providers that deliver services to in-scope financial entities, regardless of where those ICT third party service providers are located. As a result, DORA's impact on such service providers has been felt globally.

ICT services

The definition of 'ICT services' has proven particularly challenging. According to DORA, 'ICT services' means digital and

data services provided through ICT systems to one or more internal or external users on an ongoing basis. This includes hardware as a service and hardware-related services, which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.[9] DORA adopts a broad definition in order to maintain a high level of digital operational resilience and to remain responsive to technological developments.

The definition of 'ICT services' is integral to determining the scope of services subject to DORA's regulatory framework. In January 2025, Q&A 2999[10] provided a timely clarification for financial entities receiving services from other regulated firms. Q&A 2999 explains that certain regulated financial services and ancillary activities remain out of scope and are not considered ICT services under DORA. This also applies to entities regulated in third countries. However, ICT services provided by financial entities that are unrelated to, or independent of, their regulated financial services and ancillary activities should be subject to DORA.

KEY DORA REQUIREMENTS

ICT risk management framework and ICT-related incident management[11]

Financial entities must establish a framework setting out principles and requirements for a sound, comprehensive and well-documented ICT risk management framework. They must also manage ICT-related incidents and notify competent authorities of major ICT-related incidents and significant cyber threats. DORA provides a simplified ICT risk management framework for certain small and non-interconnected financial entities, recognising their more limited risk profile and operational complexity. These entities are exempt from some of the more detailed requirements under the broader DORA framework and are instead subject to proportionate obligations designed to ensure a baseline level of digital resilience.

The prescriptive nature of these requirements has compelled many firms to fundamentally reassess their existing ICT risk management frameworks. Unlike earlier regulations that set out high-level principles, DORA requires specific documented procedures and effective governance structures.

Contractual arrangement requirements and register of information

As part of ICT third party risk management, financial entities must include certain key provisions in contractual arrangements with ICT third party service providers.[12] Financial entities are also required to maintain and update, at entity level and at subconsolidated and consolidated levels, a register of information relating to all contractual arrangements for the use of ICT services provided by ICT third party service providers.[13]

Heightened contractual and register of information obligations apply where the financial entity determines that an ICT third party service provider supports 'critical or important functions'. DORA defines a 'critical or important function' as 'a function, the disruption of 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, or with its other obligations under applicable financial services law'.[14] In practice, 'critical or important functions' under DORA might be considered core financial services like payment processing, clearing/settlement, large-scale fund management and crucial customer authentication, whose failure would materially impair financial performance, service continuity or

regulatory compliance. However, the determination of what constitutes a 'critical or important function' ultimately remains with each financial entity.

It remains an ongoing challenge for financial entities to determine which ICT service providers support 'critical or important functions'. The flexibility inherent in the definition, and the lack of specific guidance on how to apply it, raises the risk for ICT service providers that certain financial entities may classify them as supporting 'critical or important functions', whereas other financial entities do not, even where the provision of services is identical. ICT service providers may express their own views on whether they support 'critical or important functions', but the final decision rests with the relevant financial entity.

Operational resilience testing[15]

Financial entities (other than microenterprises)[16] must implement digital operational resilience testing programmes encompassing a range of assessments, tests, methodologies, practices and tools. Tests must be undertaken by independent parties, whether internal or external. Internal testers must have sufficient resources and avoid conflicts of interest. They must also establish procedures and policies to prioritise, classify and remedy issues identified during testing and implement internal validation methodologies to address all identified weaknesses, deficiencies and gaps. Appropriate tests must be conducted at least annually on all ICT systems and applications supporting critical or important functions.

Additionally, certain financial entities must conduct advanced testing in the form of threat-led penetration testing (TLPT) at least every three years. TLPT covers several or all critical or important functions and simulates real-world attacks, including those targeting people and processes, as well as technical vulnerabilities. This requirement does not apply to entities subject to the simplified ICT risk management framework or to microenterprises.

MAJOR COMPLIANCE CHALLENGES

Contractual repapering exercise

One of the most significant challenges firms have faced concerns the mandatory terms that must be included in contractual arrangements governing the use of ICT services. Heightened provisions apply where the financial entity categorises the relevant ICT services as supporting critical or important functions. Many legacy contracts do not contain the required clauses, such as access and audit rights, subcontracting provisions and exit strategies. As a result, such contracts need to be reopened and renegotiated. Even where legacy contracts address some or all of the relevant issues, the contractual language is not as prescriptive or detailed as what is required under DORA.

Negotiations have been particularly challenging with noncritical ICT third party service providers who are not directly bound by DORA. Disputes often arise over which party's standard terms should serve as the starting point for negotiations, creating friction and delaying compliance efforts. The financial and operational burden has been substantial, with some firms dedicating entire teams to contract remediation for extended periods.

Building and maintaining the register of information

Another significant challenge has been building and maintaining the register of information, a central catalogue of all contractual arrangements for the use of ICT services provided by ICT third party service providers. Financial entities must maintain and update the register at entity level and at subconsolidated and consolidated levels and

submit it to their respective national competent authorities.

The technical complexity of this requirement has proven daunting. Implementing technical standards (ITS) were published to establish a single set of standard templates for the register of information.[17] However, finalising the ITS on the register of information took time. Following industry feedback, the ESAs reduced the number of data points and streamlined the templates.

One major sticking point in completing the registers has been the use of identifiers. ICT third party service providers established in the EU may use either a Legal Entity Identifier (LEI) or a European Unique Identifier (EUID). By contrast, providers established in third countries may use only an LEI. As a result, some providers have had to obtain LEIs for the first time and maintain them annually, thereby introducing additional compliance requirements.

Although the obligation to maintain and update the register of information falls to financial entities, in most cases, the information to be included in the register requires entity and subcontractor information from ICT third party service providers. In practice, such information is not always readily available, particularly where non-EU providers lack LEIs or where providers do not maintain complete visibility of subcontractors within their supply chains. Consequently, the preparation and completion of the registers prompted an extensive mapping exercise by financial entities and their ICT services providers to cover the full supply chain of subcontractors.

Additionally, from an organisational perspective, it can be difficult for a financial entity to determine who should own the register of information internally. For example, reasonable arguments may be made that responsibility should properly sit with one of several control functions, including risk, procurement, legal or technology. Furthermore, contractual data may be scattered across business units or systems, with limited visibility or standardisation. Scale also presents a challenge, as hundreds or even thousands of ICT third party service providers may need to be evaluated for inclusion, depending on the size of the financial entity.

Regulatory delays and uncertainty

One of the most widely discussed issues in the DORA implementation process was the delay in the publication of the final technical standards and guidance, the so-called 'Level 2' measures, which provided the detailed requirements necessary for financial entities and their ICT service providers to comply with the relevant principles set out in DORA. The initial lack of clarity surrounding DORA's requirements, particularly concerning Level 2 measures, created uncertainty for many financial institutions. For example, it was not until 22nd January, 2025 that the ESAs published the highly anticipated guidance prepared by the European Commission to clarify the distinction between ICT services and financial services.[18]

More broadly, delays in the publication of technical standards and guidance left many firms in a holding pattern while awaiting clarity on several fronts, resulting in delayed implementation efforts. The impact of these delays was compounded by inconsistent national implementation. In March 2025, the European Commission launched infringement proceedings against 13 EU Member States, approximately half of the EU, for failing to transpose the Amending Directive into national law by 17th January, 2025.[19] This exemplifies that timeline slippage occurred at both European and national levels.

EMERGING BEST PRACTICES AND STRATEGIC APPROACHES

The implementation of DORA has highlighted the complexity inherent in regulating

digital operational resilience across a diverse and interconnected financial services ecosystem. While the challenges have been significant, the experiences of early adopters provide valuable insights for firms still working towards full compliance.

DORA implementation is unfolding against a backdrop of accelerating enterprise cloud adoption, data-intensive operating models and the rapid integration of artificial intelligence (AI) into core processes and controls. These developments can meaningfully facilitate compliance by improving observability, automating control execution and enhancing incident detection and response. At the same time, they may introduce new dependencies, concentration risks and model governance obligations that can complicate end-to-end assurance. The practical imperative for firms is therefore to align cross-functional DORA governance with broader corporate technology strategy. This includes selecting architectural patterns and operating models that preserve auditability and exit optionality, designing data pipelines that support register of information completeness and timely incident reporting and establishing clear accountability for AI-enabled tools within ICT risk management frameworks. Positioning DORA as an enabler of strategic technology decisions, rather than as a parallel compliance workstream, has proved critical to achieving sustainable outcomes in early implementations.

We set out below our observations on emerging best practices and strategic approaches for firms navigating compliance with DORA requirements.

Establishing effective governance structures

Many firms have established a cross-functional DORA working group, creating governance structures with representatives from teams such as legal, risk, compliance, technology and operations. Other firms have appointed DORA programme leads or formed steering committees to oversee initial implementation and ongoing compliance. In either case, it is important for firms to ensure that the responsibility for DORA compliance is clearly allocated to an appropriate individual or team.

Moreover, cross-functional collaboration is essential to prevent siloed efforts, miscommunication and compliance gaps, ensuring firms are adequately staffed to meet ongoing DORA obligations.

Strategic contract remediation

To overcome the challenges associated with contract remediation, firms may develop a DORA-compliant contract clause library to be used internally in the negotiations, together with standard fall-back clauses to facilitate discussions and promote consistency in more complex cases. Firms may also prioritise remediation by tiering service providers according to criticality, for example by focusing first on those service providers supporting critical or important functions. This approach enables phased implementation and supports the development of a remediation plan with clearly defined completion timings.

Industry collaboration and knowledge sharing

Firms are collaborating with trade associations, participating in regulatory roundtables and even benchmarking strategies with peers. This allows for collective engagement on uncertain issues to understand how other firms are addressing similar challenges. It also supports the development of industry-aligned positions and helps reduce competitive disadvantage.

Board-level engagement and strategic oversight

Senior management and board engagement is essential for large regulatory initiatives such as DORA compliance. Firms may therefore include DORA compliance as a standing agenda item for risk and audit committees or other relevant governance forums. It may also be useful to produce board briefing papers with implementation timelines, risks and readiness metrics.

Preparing for testing requirements

The TLPT requirements should not be underestimated, and firms should adopt a strategic, phased approach to implementation. This may require developing standardised incident classification procedures that align with technical standards, as well as conducting dry-run tests and simulations involving ICT disruptions and third party failures. Firms should also implement comprehensive evidence logging for all tests to ensure audit readiness.

Addressing register of information complexities

To address challenges relating to the register of information, ICT third party service providers may consider providing standardised entity-level information across their financial entity relationships. This approach minimises the burden on service providers while enabling financial entities to complete relationship-specific information. ICT third party service providers should also ensure that subcontractor agreements require the provision of necessary information and permit its onward sharing with financial entities where required.

Financial entities should allocate internal responsibility for maintaining the register of information. For example, some firms have appointed 'DORA champions' to lead and manage DORA compliance. It may also be helpful for financial entities to create a central data repository or inventory platform to store the necessary information and ensure standard intake of such information during onboarding of new service providers to populate the register efficiently.

Proportionality

The principle of proportionality under DORA requires financial entities to implement DORA's requirements in a manner proportionate to their specific circumstances, size, overall risk profile and the nature of their services and operations. This avoids a 'one-size-fits-all' approach and allows for more flexible compliance based on individual circumstances. For example, large institutions providing multiple services must establish a fully developed ICT risk management framework addressing all relevant aspects of DORA's Level 1 and Level 2 measures. However, smaller entities, such as boutique trading firms, may implement a simplified ICT risk management framework covering only the areas relevant to their functions, services and industry.[20]

Technology strategy integration

Firms may consider embedding DORA considerations directly into their cloud, data and AI roadmaps. For example, data governance frameworks can prioritise the accurate and timely population of the register of information and support efficient incident classification, escalation and reporting. Risk management functions can clarify which use cases fall within ICT governance, document model risks and controls and ensure that AI-enabled monitoring augments rather than replaces human oversight. Integrating these dimensions at the design stage should reduce rework, shorten remediation timelines and strengthen evidential readiness for supervisory review.

THE FUTURE OF DIGITAL OPERATIONAL RESILIENCE

Anticipating future developments

DORA has been designed as a forward-looking framework, but the pace of technological change means it will almost certainly need to evolve over time. As new digital threats and innovations emerge, regulators are likely to revisit and update DORA's requirements to ensure they remain fit for purpose. To future-proof their operational resilience strategies, firms should focus on building adaptable and scalable frameworks rather than aiming solely for minimum compliance.

Building competitive advantage through compliance

DORA presents both a challenge and an opportunity. Firms should not consider DORA as a tick-box exercise but as an opportunity to strengthen their digital resilience. The firms that approach DORA compliance strategically will gain not only compliance but also a competitive advantage in operational integrity and trust.

CONCLUDING REMARKS

Many entities were not fully compliant with DORA's requirements by 17th January, 2025. For example, while financial entities may have initiated contract remediation discussions with ICT third party service providers, not all contracts had been updated. Firms that remain non-compliant should implement structured remediation plans and take active steps towards compliance. Successful DORA implementation requires establishing robust, sustainable processes that evolve with regulatory expectations and technological developments. Firms that invest in adaptable frameworks, cross-functional collaboration and open dialogue with regulators and industry peers will be best positioned to navigate ongoing digital operational resilience challenges.

More broadly, operational resilience is an ongoing journey that requires regular review and enhancement of controls to address emerging risks. As the financial services sector continues its digital transformation, DORA provides the foundation for a more resilient and trustworthy financial ecosystem. The lessons learned from DORA implementation underscore the importance of treating regulatory compliance as integral to business strategy. Firms that successfully integrate DORA requirements into their operational and strategic frameworks should achieve compliance while building the operational resilience necessary to thrive in an increasingly digital financial services landscape.

References

(1) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, available at https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng (accessed 3rd March, 2026).

(2) Final Report on EBA Guidelines on Outsourcing (25th February, 2019) EBA/GL/2019/02 ("Outsourcing Guidelines"), available at https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf (accessed 3rd March, 2026).

(3) In July 2025, the EBA published a consultation on new guidelines for the management of third-party risk. The new guidelines are aligned with DORA but extend to non-ICT services. They will set out how financial services firms can manage risks associated with using third parties. The new guidelines will replace the Outsourcing Guidelines. Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk (8th July, 2025) EBA/CP/2025/12, available at https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf (accessed 3rd March, 2026).

(4) EIOPA Guidelines on information and communication technology security and governance (published 12th October, 2020) EIOPA-BoS-20/600, available at https://www.eiopa.europa.eu/document/download/bfc3d846-8a2b-4ae3-ac77-fc5750cfa76d_en?filename=Guidelines%20on%20information%20and%20communication%20technology%20security%20and%20governance.pdf (accessed 3rd March, 2026). On 19th December, 2024, EIOPA revoked these guidelines to avoid duplications and overlaps with DORA. *See* available at https://www.eiopa.europa.eu/eiopa-revokes-previous-guidelines-avoid-duplications-and-overlaps-dora-2024-12-19_en (accessed 3rd March, 2026).

(5) 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 as regards digital operational resilience for the financial sector ("Amending Directive"), available at https://eur-lex.europa.eu/eli/dir/2022/2556/oj/eng (accessed 3rd March, 2026).

(6) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) ("NIS 2"), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555 (accessed 3rd March, 2026).

(7) 'Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure' 88 Fed. Reg. 51896 (4th August, 2023), available at https://www.govinfo.gov/content/pkg/FR-2023-08-04/pdf/2023-16194.pdf (accessed 3rd March, 2026).

(8) *See* Article 2(1)(k) of DORA.

(9) *See* Article 3(21) of DORA.

(10) Q&A 'Based on the definition of DORA Article 3(21), what types of services should be considered ICT services?' (22nd January, 2025) DORA030 – 2999 ("Q&A on ICT Services"), available at https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora030-2999_en (accessed 3rd March, 2026).

(11) *See* Articles 6–23 of DORA.

(12) *See* Article 30 of DORA.

(13) *See* Article 28(3) of DORA.

(14) Article 3(22) of DORA.

(15) *See* Articles 24–27 of DORA.

(16) "Microenterprise" means a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million. *See* Article 3(60) of DORA.

(17) *See* Commission Implementing Regulation (EU) 2024/2956 of 29 November 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to standard templates for the register of information, available at Eng.

(18) *See* Q&A on ICT Services.

(19) *See* European Commission's press release (27th March, 2025) 'Commission Calls on Member States to Fully Transpose the Digital Operational Resilience Act (DORA) Directive', available at https://ec.europa.eu/commission/presscorner/detail/fi/inf_25_761 (accessed 3rd March, 2026).

(20) *See* Article 16 of DORA.