afme/ Finance for Europe

MUREX

DORA: a Tech Perspective on Streamlining Implementation

July 2025

Association for Financial Markets in Europe
www.afme.eu

Foreword

On 17 January 2025, the Digital Operational Resilience Act (DORA) came into effect, signifying a major step up for risk management within financial services across Europe. The obligations under DORA, while directed at financial entities (FEs), have important implications for the third-parties that provide information and communications technology services to the sector, many of which are not based within the EU. In this thought leadership piece, AFME and Murex identify several areas where tech providers can support the effective implementation of DORA, including through collaborative approaches in partnership with the financial sector.

The proposals reflect the experiences of AFME members from the ongoing implementation of DORA but should not be construed as formal endorsement. Rather, the proposed avenues expose potential areas for future discussion and further exploration. In certain cases, the proposals represent longer term goals which would require an amendment to DORA's legal text. The paper incorporates the views of Murex, a software provider with market exposure in trading, operations and risk management. This includes drawing on the insights of the Murex CISO, Thibaut Bachelier, who presented to the AFME Technology & Operations Committee at its annual Paris meeting on 30 April 2025.

Disclaimer

This document is intended as thought leadership only and is not intended to be and should not be relied upon as being legal, financial, investment, tax, regulatory business or other professional advice. AFME does not endorse the proposals in this paper but presents them as areas for further discussion and appraisal.

Summary

It is within DORA's so-called "third pillar" that the ramifications for ICT third-party providers are primarily set out. Its inclusion within the regulation reflects a global supervisory focus on the financial sector's supply chain dependencies. DORA not only imposes contractual safeguards on a bank's relationship with its tech suppliers, but also brings some of those players within the regulatory perimeter.

The latter is achieved via the incoming Critical Third-Party Provider (CTPP) regime, by which the European Supervisory Authorities (ESAs) are due in the second half of 2025 to designate certain tech providers as "Critical", in light of their concentration risk and lack of feasible market substitutes.

Yet DORA's other pillars, namely the Risk Management Framework for banks; the harmonised obligations on incident reporting; the evolution of resilience testing; and the creation of information sharing forums all have additional implications for providers. In certain instances, DORA directly stipulates the relationship between FE and provider, but in many others the door is left open for further collaboration. This paper highlights five of these opportunities:

Areas for Collaboration between Banks and Providers

1. Compliance Audits & Accredited Providers
2. Security Awareness Training
3. Operational Resilience Testing
4. Incident Reporting
5. Cyber Intelligence & Information sharing

Avenue 1: Compliance Audits & Accredited Providers

DORA requires FEs and their senior management to conduct audits as to the state of compliance within both their own business and the wider supply chain. This reflects a long-standing risk-management practice, with audits rights designed to support an FE's ability to oversee, monitor and ensure the regulatory compliance of third-party arrangements on a risk-based approach (i.e., at a frequency commensurate to the level of risk of the engagement).

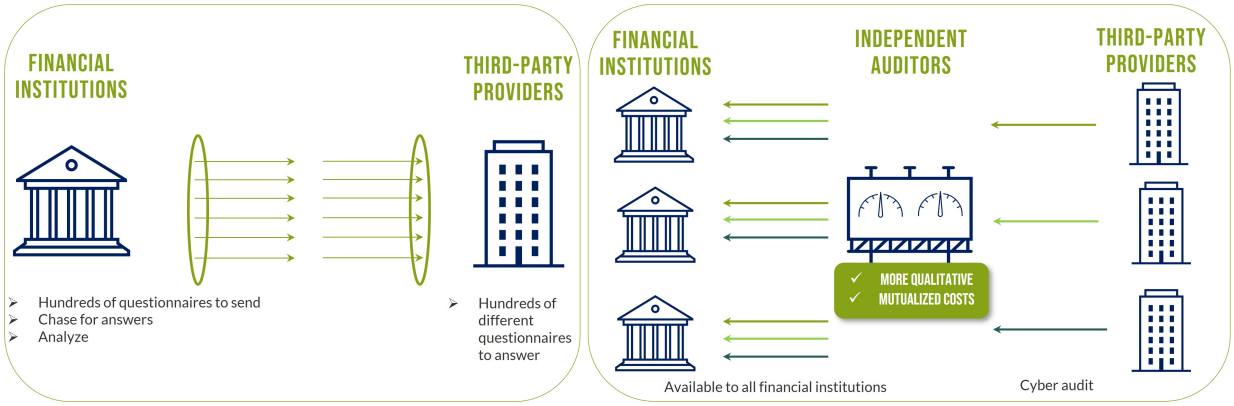
Through the Level 1 text of DORA, and related technical standards, supervisors have set out the level of expectation, with FEs required to pre-determine the frequency of audits and inspections as well as the areas to be audited, adhering to commonly accepted audit standards, and in line with any supervisory instruction. In parallel, providers are obligated to fully cooperate during inspections and audits with both the FE and if relevant the authorities themselves. Typically, the conditions under which such collaboration is provided can be determined on a case-by-case basis or by contractual arrangement.

Audit and access rights are a key mechanism through which financial entities discharge their oversight responsibilities under DORA. However, their application can pose operational challenges for third-party providers – particularly when multiple financial entities seek to exercise these rights at any one time. This challenge highlights the need for proportionate and coordinated approaches.

Third-Party Risk Management (TPRM) questionnaires are a good illustration as they have become a common, though increasingly burdensome, practice in the financial sector. Under Article 8(7) of DORA, financial entities are required to conduct specific ICT risk assessments on their systems at least annually. This regulatory obligation is expected to drive even greater reliance on TPRM questionnaires as a substitute for more resource-intensive full audits.

While these questionnaires serve a purpose in due diligence, the process can be declarative and often requires additional checks to assess the cyber risk maturity of the individual third-party provider. There is support amongst the third-party provider population to reduce the operational burden, whilst ensuring that FEs are able to meet regulatory expectations and supplier assurance.

A shift toward mutualised and more qualitative assessments conducted by independent and accredited third parties could be part of this solution. This would not only reduce redundancy but also enhance the reliability of the evaluations. In some cases, particularly for providers designated as Critical Third-Party Providers (CTPPs), it may be appropriate for such audits to involve supervisory authorities like the ESAs or competent authorities (CAs), given the systemic risk these entities may pose. Any developments will nonetheless still need to ensure that third-party solutions or independent reports reach the assurance requirements for each respective FE, which may differ according to each institution.



This approach would better align with DORA's objective of strengthening operational resilience across the financial ecosystem by ensuring that oversight mechanisms are both meaningful and proportionate.

Over time this could even lead to the development of accreditations, whereby providers who have been subject to audits, especially external audits executed by third parties, could leverage the exercise as effective certification which other FEs could rely upon for demonstrating DORA compliance. This resembles the presumption of conformity, which is embedded in the Cyber Resilience Act, whereby firms can use the ENISA cybersecurity certifications as assurance that the providers of those services have met the necessary level of cyber risk management.

Avenue 2: Security Awareness Training

A shorter term, and arguably more readily available avenue for collaboration lies in DORA's obligations on security awareness training. Under these provisions, FEs must develop programmes for the training of employees to ensure that risk management is not siloed within operational teams, but widely understood and demonstrated across the firm.

The programmes and training apply to all employees and senior management, though they can vary in technical complexity in relation to the role of the individual. The application of such training within firms is well established but with DORA there is an additional push to actively consider and bring on-board third-party providers. This can even amount to having joint training with participation from employees from the provider where appropriate.

Those firms which wish to take a more proactive approach to DORA compliance could also seek to leverage the technical expertise of respective providers as part of this collaboration. For example, DORA expects FEs to monitor technological developments on a continuous basis, with a view to understanding the possible impact on digital operational resilience. Seeking input from providers as part of the training, including lessons learnt from other clients, would be a resource-effective way of broadening the firm's line of sight and ensuring that the vulnerabilities facing the supply chain are fully factored into an FE's own security awareness training.

Avenue 3: Operational Resilience Testing

DORA represents a significant enhancement in operational resilience testing. The breadth of the obligation on FEs is represented in the range of tests which are outlined within the regulation. This encompasses:

- vulnerability assessment and scans
- open sources analyses
- network security assessment
- gap analyses
- physical security reviews
- questionnaires and scanning software solutions
- source code reviews
- scenario-based tests
- compatibility testing
- performance testing
- end-to-end testing.

As indicated above, authorities are increasingly keen for third-party provider participation within an FE's testing. Given the variety of testing mandated, some of which entails high levels of technical specialism, there is significant benefit to both from facilitating this in practice.

With the adoption of managed services continuing to grow, there has been an increase in the delegation of the configuration, management, and provisioning of aspects of FE IT infrastructure to third-party providers. In this context, it would be mutually beneficial for both financial entities and their service providers to reconsider how technology testing is approached.

Specifically, third-party providers may be better equipped to test the common technology components they deliver across multiple institutions.

To ensure transparency and maintain trust, the involvement of an external and independent testing body could be considered. This third party would provide standardized, verifiable proof of testing outcomes to each FE relying on the provider, particularly when the services support one or more critical functions. This approach would allow financial institutions to redirect their focus toward testing activities that are more specific to their internal processes and operational workflows.

Such a collaborative model would not only reduce redundancy and improve resource allocation, but also enhance the overall quality and consistency of testing across the financial ecosystem. It would also facilitate wider adoption of the intention within DORA to pursue greater mutual recognition of testing results.

One of the most resource intensive forms of testing is Threat-Led Penetration Testing (TLPT). The real-time simulation is both invasive in terms of a firm's systems and applications, and lengthy in duration, but it is a form of testing which globally significant banks have long been familiar with, at least in the EU under the TIBER framework. The

novelties in DORA relate to the extension in TLPT scope to include third-party providers, and potentially even other FEs (pooled TLPT).

The challenge in this extension of scope is how to maintain the value of a TLPT exercise, in terms of its depth and access to internal infrastructure and data, while ensuring confidentiality over sensitive information. It is for this reason that AFME has considerable concern over the feasibility of pooled TLPT, and fears it may result in a shallow, non-probing exercise with limited risk management value.

On the other hand, joint TLPT, containing only one FE and a provider, presents greater feasibility.

Voluntary participation by third-party providers in TLPT might in fact offer operational and strategic benefits. It might enhance the overall value of the exercise by contributing depth and quality to the testing process, which in turn, promotes consistency and helps optimise long-term testing costs. However, these benefits can only be fully realized if each party's contribution to TLPT is well-structured.

Given that coordination is key, one potential solution could be to mandate a single, annual TLPT exercise for CTPPs, coordinated by an independent body. This would foster greater trust and alignment across the industry.

Avenue 4: Incident Reporting

Under DORA, the ECB was commissioned to undertake a feasibility study into a DORA incident reporting hub. The study, which was published in January 2025[1], uncovered two possible models:

- A data-sharing hub, which would collate onward transfers of incident reports from a single competent authority
- A centralised hub, which would serve as the sole recipient of industry reports and remove the need for duplicate reports to various authorities in multiple member states

While the feasibility study uncovered possible risks, for example that cyber-criminal would seek to target the hub itself as a golden source of information, the ECB concluded there was merit in further analysis.

Should a DORA incident reporting hub come to fruition, there is obvious rationale in ensuring that it serves also as the conduit or recipient of incident reports from the third-party providers who are in future to be designated as critical.

[1] https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-study-feasibility-further-centralisation-major-ict-related-incident-reporting-financial

Avenue 5: Cyber Intelligence & Information sharing

The fifth and final pillar of DORA relates to information sharing, with FEs encouraged to exchange cyber threat information and intelligence, in order to raise awareness and support defence capabilities for the sector as a whole. These provisions must be welcomed as an area ripe for proactive development given the growing prevalence of cyber attacks and the appeal of financial services to malicious actors.

The information sharing provisions are largely set out within Article 45. This clarifies that while voluntary, information sharing should be facilitated within an established trusted community of financial entities, with notification to authorities of its set-up and with safeguards for protecting the sensitive nature of the information.

DORA explicitly acknowledges that once these communities have been established there could be merit in inviting providers to participate. This reflects developments within the UK, where the Bank of England has jointly created with industry a number of forums for information sharing within the Sector Response Framework. The UK is already proposing to draw into these forums the UK's Critical Third Parties once designation by HM Treasury has been undertaken.

Many tech providers will have deep insights on the latest trends within the cyber threat landscape from their products and services on threat detection, and from their engagement in industry testing. Providers could also be invited to participate in order to share insights on attacks directed at them, particularly those which caused onward disruption. While acknowledging this is a longer-term avenue, it is one which must surely benefit not only both parties, but the wider sector.

Conclusion

DORA has represented a major milestone in risk management and digital resilience within financial services. The tight timeframes for implementation, with a number of technical standards being finalised after the Go-Live date of 17 January 2025, have resulted in considerable operational pressure on financial entities. This is likely to permeate throughout the first year of DORA, as third-party remediations continue and the first DORA testing exercises are launched.

Once though the dust settles, it is clear that DORA does have the potential to unlock a more collaborative and transparent ecosystem that reflects the growing importance of tech providers within the financial industry. AFME and Murex hope this short paper spurs further discussion of the avenues available.

Contacts

AFME

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

Murex

Murex provides enterprise-wide, cross-asset financial technology solutions to sell-side and buy-side capital markets players. With more than 60,000 daily users in 65 countries, its cross-function platform, MX.3, supports trading, treasury, risk, post-trade operations, as well as end-to-end investment management operations for private and public assets. This helps clients better meet regulatory requirements, manage enterprise-wide risk, and control IT costs. Learn more at www.murex.com

Thibaut Bachelier
Chief Information Security Officer
tbachelier@murex.com

Mickaël De Oliveira Neves
Market & Regulatory
Intelligence Manager
mdeoliveiraneves@murex.com

afme/
Finance for Europe

London Office
Level 10
20 Churchill Place
London E14 5HJ
United Kingdom
+44 (0)20 3828 2700

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0)2 883 5540

Frankfurt Office
Große Gallusstraße 16-18
60312 Frankfurt am Main
Germany
+49 (0)69 710 456 660

Press enquiries
Rebecca Hansford
rebecca.hansford@afme.eu
+44 (0)20 3828 2753

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

AFME is registered on the EU Transparency Register, registration number 65110063986-76