The Digital Operational Resilience Act (DORA) and Third-Party Risk Implications

Authors:
Gustavo Pregoni, Director Risk and Compliance, Probus Insurance Company Europe DAC and Member of Compliance Institute's Prudential, Regulation and Governance (PR&G) Working Group.

Darryl Lynch, Enterprise Risk, U.S. Bank Europe DAC and Member of Compliance Institute's Prudential, Regulation and Governance (PR&G) Working Group.

Tom Brennan, formerly Head of Risk & Regulatory at EisnerAmper Ireland and Chair of the Compliance Institute's Prudential, Regulation and Governance (PR&G) Working Group.

Deirdre O'Reilly, Independent Non-Executive Director and Member of Compliance Institute's Prudential, Regulation and Governance (PR&G) Working Group.

In consideration of the fact that financial entities have long relied - and continue to do so - on outsourced arrangements with third-party service providers for the provision of Information and Communication Technology ("ICT") services, this article explores the key aspects of DORA impacting firms' third-party risk exposure.

To this extent, the relevant implications of the new requirements on the sound management of ICT third-party service providers by financial entities are hereby articulated, not only under a key contractual provisions' perspective but also through the lenses of alignment with standards and guidelines already in place.

1. What is DORA and its objective

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act, "DORA")[1] entered into force on 16 January 2023 through publication in the Official Journal of the European Union and will apply from 17 January 2025.

DORA is intended to promote a coherent approach to the digital operational resilience of both financial entities in the EU and their ICT third-party service providers, through the creation of a harmonised regulatory and supervisory framework across Members States, capable of countering the vulnerabilities to cyber threats of the overall financial sector.

It considerably strengthens the requirements for in-scope entities to establish a sound, comprehensive and documented ICT risk management framework to effectively address ICT risk and the classification and reporting of related incidents, including the provision of additional requirements for managing ICT third-party risk, defined by DORA Article 3(18) as "the risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements".

Other key pillars of DORA are related to the introduction of general requirements to perform digital operational resilience testing; a newly developed oversight framework applicable to critical ICT third-party service providers; and provisions governing information sharing arrangements on cyber threat information and intelligence.

2. Scope of Application

DORA applicability includes financial entities such as credit institutions, stock exchanges and clearing houses, alternative fund managers, management companies, (re)insurance undertakings, payment institutions, electronic money institutions, as well as payment service providers, cryptocurrency, crypto-asset issuers and token issuers.

However, its scope of application extends also to those ICT third-party service providers which the three European Supervisory Authorities ("ESAs") - acting through an established Joint Committee -designate as "critical" in accordance with DORA Article 31.

Various exemptions from DORA's scope of application apply to very small enterprises, so called "microenterprises", defined as financial entities which employ fewer than ten persons and have an annual turnover and/or balance sheet total does not exceed EUR 2 million. In addition, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries qualifying as small (fewer than 50 persons and annual turnover / balance sheet not exceeding EUR 10 million) or medium-sized (fewer than 250 persons and annual turnover / balance sheet not exceeding EUR 50 / 43 million respectively) enterprises are exempt from DORA.

The proportionality principle will also apply, taking into consideration size and overall risk profile of the firms together with the nature, scope and complexity of the relevant services, activities and operations (please refer to DORA Article 4).

3. Sound management of ICT third-party risk

Firms who invested heavily in the implementation of the Cross Industry Guidance on Outsourcing ("CBI Outsourcing Guidance"[2]) and the Cross-Industry Guidance on Operational Resilience ("CBI Operational Resilience Guidance"[3]) both issued by the Central Bank of Ireland in December 2021 should be able to leverage that work in meeting the requirements of Article 28 of DORA.

3.1 General Principles

One of the key aspects of DORA is the management of risks posed by third parties, including outsourced ICT service providers. This is addressed by Article 28 of DORA which requires firms to manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework in accordance with the following principles:

a) have in place contractual arrangements for the use of ICT services;
b) manage ICT third-party risk in light of the principle of proportionality , taking into account:
   i. the nature, scale, complexity and importance of ICT-related dependencies; and
   ii. the risks arising from contractual arrangements taking into account the criticality or importance of the respective service and the potential impact on the continuity and availability of financial services and activities.

3.2 Risk Management Strategy

Firms overall outsourcing strategy should have been documented and Board approved under the CBI Outsourcing Guidance and should align to the regulated firm's business strategy, business model, risk appetite, and risk management framework. In addition, the strategy should consider:

- the extent of outsourcing;
- activities to be outsourced;
- risks arising for such arrangements (and how these are managed); and
- the extent to which the firm has skills and capacity to monitor and exercise oversight of outsourcing arrangements.

The CBI Outsourcing Guidance requires the strategy to consider what ICT services and operations firms are retaining within the organisation and the different risks associated with ICT outsourcing, particularly in the case of cloud-based offerings.

In preparing for DORA, firms should review this strategy and amend where necessary to meet the DORA requirements.

Article 28 (2) of DORA requires firms to properly manage / have "a strategy on ICT third-party risk risks" for critical or important functions. The Board shall "regularly review the risks identified in respect to contractual arrangements on the use of ICT services supporting critical or important functions".

DORA's emphasis on ICT risk management requires firms to have a comprehensive ICT risk management framework. How this is implemented and integrated into existing risk management frameworks will depend on the nature, scale and complexity of the firm and area of focus during DORA implementations.

The regulation also mentions that, where applicable, the strategy should take into account the multi-vendor strategy i.e. where feasible, firms should be aware of potential concentration risk and avoid becoming overly reliant on a single ICT third-party service provider.

3.3 Register of Information

Article 28 (3) of DORA requires firms to have a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers, which shall make available to the competent authority, upon its request.

This requirement complements existing arrangements introduced by the CBI in 2022 requiring firms with a PRISM Impact Rating of Medium-Low or above to establish an outsourcing register in a prescribed format for annual submission to the CBI.

When implementing the CBI Outsourcing Guidance, many firms opted to use this CBI mandated template format as their internal outsourcing register to avoid possible duplication / potential conflicts of having two registers. Similarly, many PRISM Impact Low rated firms adopted these CBI templates in anticipation for any potential CBI request to view the register.

Firms should be able to review the new DORA requirements and use a certain amount of information already present into their existing outsourcing register, although on January 10, 2024, the ESAs published their Draft Implementing Technical Standards ("ITS") on the standard templates for the purposes of the register of information[4]. The final RTS for the information register is expected to be adopted by the European Commission in the near future.

The standard templates of the register of information are proportionate by design as the scale of information is subject to the contractual relationship on ICT services with ICT third-party service providers. Therefore, an in-scope entity relying on a significant number of ICT third-party service providers or a complex level of ICT dependencies has more information to report in the register of information than a regulated entity depending on a small number of ICT third-party service providers.

3.4 Contractual Arrangements

Preliminary Assessment

DORA imposes and obligation on firms to conduce due diligence before entering into contractual arrangement on the use of ICT services (Article 28 (3)). Importantly this is not just for a critical or important function as this is an assessment that needs to be done before that determination is made. This review should ensure service providers comply with appropriate information security standards.

Firms are also required to have rights to terminate contracts in certain circumstances, monitoring and audit rights, and exit strategies should the need arise. While many firms did review ICT service contracts as part of the 2021 CBI Outsourcing Guidance implementation, it is recommended that ICT critical or important contracts be reviewed to ensure they meet these DORA requirements and any identified gaps properly addressed.

4.Key Contractual Requirements

Following on the previous paragraph, contracts are a key component to managing third-party arrangements. In DORA, the criticality of the third-party service provider proportionally influences the contractual clauses and obligations a third-party service provider must adhere to. For example, all contracts must describe the services rendered, the locations in which activities are performed, co-operation with regulatory agencies and termination rights. However, contracts of critical ICT third-party service providers must include clauses containing performance targets with agreed service level agreements, notice periods, and participation in audits or penetration testing.

Subcontracting is also an area of focus within DORA, as it can have a material impact on the service rendered, as seen with recent technology-related market events. Where a critical service is subcontracted by the third-party, additional contractual clauses are required, including details of the subcontractor(s) itself and also that the third-party service provider commits to performing certain risk assessments on the subcontractor(s).

Developments in this space are still subject to change as the Final Report on subcontracting under Article 30(5) ("JC 2024 53")[5] was published in July 2024 and will enter into force 20 days following its publication in the Official Journal of the EU.

5. Criticality: Assessment and Oversight

DORA requires financial entities to conduct a risk based due diligence on ICT third-party service providers before entering into any third-party relationship that includes focusing on the criticality of the outsourced services. The due diligence includes the provider's ability to deliver services without disruption, their security measures, and their track record of operational resilience.

Criticality refers to the significance of an ICT third-party service provider for the financial sector's stability and operational integrity (expressed as degrees of criticality). Providers are considered critical if their failure or disruption could significantly impact financial entities, or the wider financial market.

A criticality assessment involves both quantitative and qualitative criteria to determine which ICT third-party service providers poses a systemic risk. Factors such as the scale of services provided, the number of financial entities relying on them, and the potential for service disruption to impact the (financial) market are taken into account. This assessment ensures that financial entities can pre-emptively address risks associated with critical ICT providers.

Designated critical ICT third-party service providers are subject to a robust oversight framework. This requires ongoing monitoring of the providers' operations, assessing their risk management practices and resilience measures.

The ESAs are tasked with oversight of the critical ICT providers, ensuring compliance with prescriptive resilience standards and incident reporting requirements. Regular audits, inspections, and evaluations of service continuity plans are also part of the oversight process. Oversight also extends to ensuring that providers address any vulnerabilities or deficiencies identified during criticality assessments.

It is noted that the Joint ESAs comments on criticality assessment and oversight in DORA emphasised a holistic approach to evaluating critical ICT third-party service providers. Their proposal outlines the following two-steps:

a) Quantitative indicators with minimum relevance thresholds, aimed at evaluating providers on their systemic impact and financial entities' reliance on their services. The ESAs stressed that these indicators should be considered collectively to avoid narrow interpretations of criticality.
b) Qualitative factors to further refine the assessment, providing a more granular review of providers flagged in Step 1.

The ESAs' response acknowledged the need for proportionality and pragmatism. This includes calls from market participants to ensure that oversight mechanisms do not overly burden smaller ICT third-party service providers. The response further suggests that any designated critical entity should remain under consistent oversight, even if they temporarily fall below the indicated thresholds, to ensure continuity and mitigate systemic risks.

6.Key Takeaways

As DORA will become effective on 17 January 2025, in-scope firms should already have commenced the relevant activities to ensure compliance with requirements and guarantee their ability to uphold resilient operations in the occurrence of ICT and cybersecurity disruptions.

Some key takeaways for your firm's considerations related to third-party risk management are as follows:

- Establish a comprehensive strategy for manging ICT third-party risk, fully aligned to your firm's business strategy, business model, risk appetite and overall risk management framework.
- Identify the (non)-critical ICT third-party service providers, in accordance with the level of risk they pose and with your firm's function(s) they are providing support to.
- Maintain a complete Register of Information, outlining required information on all ICT services contractual arrangements entered by your firm.
- Stand up systems and develop processes to oversee the monitoring of any resiliency or contractual targets, inclusive of a vigorous approach to audit reviews.
- Conduct a risk based due diligence on ICT third-party service providers before entering into any third-party relationship and regular reviews of adherence to agreed service levels.
- Adopt a "contracts plus" approach whereby processes such as risk assessments, risk monitoring and stakeholder engagement complement the mutual agreements entered upon contractual sign-off.
- Assess the presence and/or the complexity of any subcontracting chain between the ICT third-party service provider and subcontractor(s).

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 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=EN
2. Central Bank of Ireland Cross-Industry Guidance on Outsourcing - December 2021 https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp138/cross-industry-guidance-on-outsourcing.pdf
3. Central Bank of Ireland Cross-Industry Guidance on Operational Resilience - December 2021 https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cross-industry-guidance-on-operational-resilience.pdf?sfvrsn=bd29921d_5
4. ESA's Final Report on the Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554 https://www.eba.europa.eu/sites/default/files/2024-01/30b47816-8d6d-432f-8dbd-b900c4306cf4/JC%202023%2085%20-%20Final%20report%20on%20draft%20ITS%20on%20Register%20of%20Information%20%281%29.pdf
5. ESA's Final Report on the Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554 JC 2024-53_Final report DORA RTS on subcontracting.pdf (europa.eu)