

Operational Resilience in the EU: Unlocking Synergies, Cutting Complexity

Key recommendations:

- **Standardize contractual terms** on operational resilience under DORA/NIS2.
- **Introduce accredited audit regimes** under DORA/NIS2 based on standards agreed and jointly developed by ESAs.
- **Simplify ROI reporting requirements** under DORA by excluding low-impact contracts, simplifying function identifiers, and introducing annual reporting of high-level suppliers.
- **Exclude functions legally required to be performed by a TPSP or typically performed by a supervised enterprise** from the EBA Guidelines on outsourcing.
- **Recognize the exclusion of regulated financial services**, including **ancillary services** provided by licensed financial entities to other financial entities, from the scope of EBA Guidelines on outsourcing.
- **Leverage third-party supplier audits** in a standardized and widely recognized format, such as ISO certification for example.

Why Resilience Matters?

Operational resilience has evolved from a strategic advantage into a **fundamental necessity** in today's interconnected and digitized economy. It should be understood as an organization's ability to **protect and sustain the core business services** that are key to its customers – especially at times of operational stress¹.

Regarding services that have become vital to customers or segments of the market, particularly in the financial industry, it is of fundamental relevance to properly address the ever-increasing complexity of operational risks resulting from relationships with service providers.

With the goal of mitigating cybersecurity and operational risks, European regulators introduced two landmark frameworks: (i) the **Digital Operational Resilience Act** (DORA); and (ii) the **Network and Information Security Directive 2** (NIS2). According to DORA, regulated entities must ensure their contractual relationship with **third-party ICT service providers** covers comprehensive cybersecurity requirements, audit and termination rights, and processes to closely monitor those providers. While NIS 2 does not explicitly address contractual

¹ PwC Report: Operational resilience: get ready for the unexpected ([Link](#))

requirements, it mandates that essential and important entities address cybersecurity risks in their supply chains. This makes it practically necessary for entities to agree on specific contractual terms with their service providers.

Most recently, the European Banking Authority (EBA) proposed Guidelines that would regulate how financial entities manage the **non-ICT risks from third-party service providers** (TPSPs).

Efforts by the regulators have significantly contributed to properly addressing operational risks, but some requirements across different operational resilience frameworks remain misaligned and cost-ineffective.

This not only **increases the compliance burden**, but it is in sharp contrast with the European Commission's **simplification and burden reduction agenda**. The Commission pledged to reduce the regulatory burden by **at least 25% for all businesses**² by streamlining procedures, eliminating overlaps, and cutting administrative costs.

Therefore, there is a **significant potential** for **achieving synergies** through more simplified and standardized approaches that would reduce the regulatory burden and boost competitiveness, without compromising on high standards.

Streamlining DORA/NIS 2 compliance

The ICT service provider landscape is characterized by a **high degree of concentration**. Numerous financial institutions (20.000 DORA regulated entities and 100.000 NIS2 regulated entities) engage in negotiations over almost **identical contractual and operational arrangements** with the same limited set of providers.

For example, thousands of small and middle-sized companies have to negotiate with and enforce DORA annexes onto sizably larger ICT service providers such as the recently designated critical ICT service providers³. The drafting and negotiations of contracts may entail considerable legal fees that especially burden SMEs.

While larger ICT service providers have developed standardised contractual frameworks to address DORA compliance of their customers that are financial entities, individual negotiations often continue to take place – **driving up costs** across the industry.

High synergies would be realized if **contractual terms on operational resilience** could be **standardized**, reducing the costs of individual negotiations and levelling potentially disparate negotiating powers. The service provider, in turn, would be subject to uniform contractual terms.

Furthermore, **risk oversight** should be harmonized through **accredited audit regimes** based on agreed standards by competent authorities. Developing **joint ESMA-ENISA auditing standards** would promote more efficient and coherent oversight, also enhancing alignment between the DORA and NIS2 frameworks.

While DORA already foresees the possibility of pooled audits, accredited audit regimes would allow service providers to mandate an **annual audit** by an **accredited audit firm** and to provide the results to its respective **regulated service receivers**. This would be a significant

² European Commission: Simplification Agenda ([Link](#))

³ Find the full list of ESAs designated critical ICT service providers under DORA [here](#).

improvement in comparison to thousands of entities trying to execute the same audits on the same dozen providers.

Simplifying DORA Register of information

DORA Register of Information (ROI) was intended to identify and oversee the critical ICT providers on the EU level, by collecting data and publishing a list of providers based on submitted registers. However, the current ROI template prescribes **95 data fields for each supplier contract** and depending on the number of contracts and sub-contracts, submissions can amount to **hundreds of thousands of rows**.

For instance, a Central Securities Depository (CSD) must list sub-services as stand-alone licensed activities, multiplying function identifiers and entries. The implementation costs alone have been reported at seven digits, with ongoing maintenance and reporting adding further expense to the industry.

By introducing **a materiality threshold** (e.g., based on contract value) to exclude low-impact contracts from the ROI reporting, or **simplifying function identifiers**, such as consolidating CSD sub-services under a single category, unnecessary reporting costs would be significantly reduced without compromising oversight.

In a further step, in line with the Commission's simplification and burden reduction agenda, regulators could **clarify the "ad-hoc basis"** for reporting requests to avoid unrealistic timelines that increase complexity and consider **annual reporting of a high-level supplier** list rather than thousands of rows of granular contractual details.

Rethinking EBA's Approach to Third-Party Oversight

The proposed EBA Guidelines would **significantly expand the scope of services** subject to regulatory requirements. Almost all **non-ICT third-party arrangements**, including intragroup third-party service providers, would fall within the scope.

The Guidelines would not only cover material non-ICT services but also extend to the procurement of other third-party services which **do not have a material impact** on financial entities' risk exposures or their operational resilience (e.g., *"Advertising & Marketing"*, *"Document Management & Archiving"*, *"Postal services & Mailing"*, *"Talent acquisition & hiring"*, as well as *advisory services*).

Significant expansion in scope would not only result in high costs for the regulated entities, which would need to perform the required risk assessment, negotiate contractual terms and perform the monitoring for these providers, it could also lead to many suppliers not being able to provide services to financial entities anymore. For example, a small marketing agency may not have the resources to comply with numerous and stringent regulatory requirements.

Such expansion runs counter to the Commission's simplification agenda, placing a disproportionate burden on financial entities and their supplies (especially SMEs), without delivering commensurate resilience benefits.

To avoid a significant increase of the regulatory burden, the Guidelines should **explicitly exclude** functions that are either **legally required to be performed by a third-party service provider** or are **typically performed by a supervised enterprise** and are not regularly carried out by the financial entities themselves. Examples include, but are not limited to, the use of central bank

functions, liquidity lines, or publicly accessible (also fee-based) data from market information providers (e.g., rating agencies).

Likewise, services provided by financial institutions for another financial institution should also be out of the scope, as those services are regulated by extensive sectoral frameworks.

Moreover, to ensure consistency of *non-ICT services* with the interpretation of *ICT services* under DORA, the Guidelines should confirm that **regulated financial services**, including **ancillary services** provided by licensed financial entities to other financial entities, are **not in scope**. These services are already subject to **robust sectoral regulation**, guaranteeing a high level of operational resilience and management of the risks associated with the provision of the respective financial services.

As the scope of covered non-ICT services is broad in nature and thus contractual requirements may diverge largely, it is even more important that financial entities are in a position to adapt contract requirements on a risk-based basis rather than to implement mandatory contractual requirements which may not suit the individual requirements.

Lastly, it would be highly cost-inefficient if each financial entity were required to conduct its own supplier audits. Instead, **third-party audits** should be leveraged in a **standardized and widely recognized format** – preferably aligned with the established frameworks such as ISO certification. This would reduce unnecessary costs to the industry without jeopardizing industry-wide resilience.

However, we caution against introducing eligibility criteria that could limit the pool of eligible providers to only those who are certified to provide services to the financial sector; or that could lead to unjustified cost premiums charged by financial industry-certified service providers.

Conclusion

Nearly a year after DORA came fully into force, the financial industry faces tangible challenges to negotiate DORA mandated annexes with third-party ICT service providers. Only approximately **20-30% of major financial institutions** report **near-complete compliance**⁴. Around **50-60%** are still in **intermediate stages**, having implemented core ICT risk management but not advanced testing or third-party oversight.

If left unchanged, the proposed EBA Guidelines are likely to follow a similar trajectory – delayed implementation driven by an overly broad scope, costly implementation and costly audit requirements.

Operational resilience should, therefore, be front and center of the Commission's simplification and burden reduction agenda. To deliver on its pledge to cut regulatory burden by 25%, regulators must move beyond fragmented frameworks and overlapping obligations.

To truly unlock the potential of operational resilience in the EU, regulators should implement harmonized contractual standards, accredited audit regimes, simplified ROI reporting requirements, and clear scope limitations that will not only reduce administrative costs but also enhance systemic resilience and competitiveness.

⁴ Deloitte: European Survey on DORA 2025 ([Link](#))