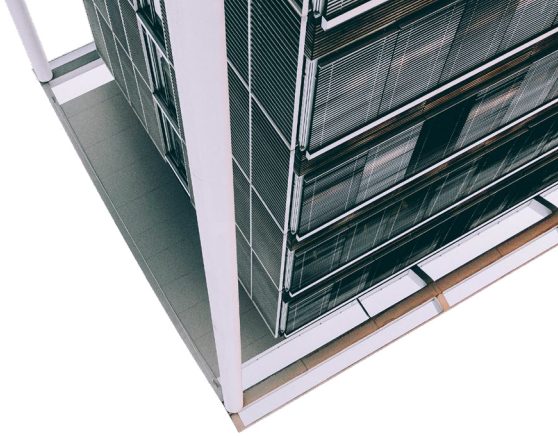
We manifest change.



White Paper

Refining DORA Compliance in 2025

Key Considerations

MONOCLE

The Digital Operational Resilience Act (DORA) was developed to enhance information and communication technology (ICT) security throughout the European Union (EU) financial sector and entered into force on 17 January 2025. The implementation of DORA required a particularly tight turnaround, with some organisations still conducting their gap analysis six months before the deadline.[1] Additionally, many financial organisations have experienced costly compliance implementations, with one report by research firm S&P Global highlighting that some firms had spent upwards of $100 million.[2]

Refining DORA Compliance

With financial institutions facing the pressure of DORA compliance, many will have implemented minimum viable solutions to meet the January 2025 deadline and will now need to review and refine their DORA frameworks over the next few months. For many, their implementations over the last few months will have revealed a clearer understanding of both the DORA requirements and long-term operating model updates that may include complex system development and vendor product implementation.

Monocle has identified three critical areas for financial institutions to review and refine. By focusing on these topics first and allocating sufficient resources to ensure these deliverables are met as soon and as effectively as possible, financial institutions can set themselves up to achieve long-term and meaningful compliance:

1 Assess the Organisation's Current State of DORA Compliance

Many of DORA's requirements overlap with existing operational risk requirements (e.g. NIS2, GDPR, MiFID II, and various operational risk and resilience guidelines), which may result in duplication of efforts, process inefficiencies, and, in the worst-case, unidentified gaps within the compliance framework. Therefore, Monocle recommends performing a gap analysis across the impacted people, processes, policies, and systems to accurately identify inefficiencies and deficiencies to be remediated throughout 2025.

Through a risk-based approach, institutions should rank deficiencies, prioritising gaps based on criticality, regulatory impact, and potential business disruption. The management body is required to approve and oversee the remediation of these deficiencies while a dedicated operational resilience working group should take responsibility, along with dedicated business stakeholders, to remediate these deficiencies. Executive management and the Board must also receive regular progress updates and track full compliance closely to avoid a loss of momentum which is common with large regulatory initiatives post go-live.

"For many, their implementations over the last few months will have revealed a clearer understanding of both the DORA requirements and long-term operating model updates that may include complex system development and vendor product implementation."

2 Enhance Inventories of ICT Assets and Third-Party ICT Service Providers

While most banks will already have some form of registry solution in place, the additional requirement to identify critical functions, identify all processes linked to third party service providers, as well as map all key links and interdependencies, requires a substantial administrative effort to effectively implement, often encountering ambiguous and complex scenarios. These information registries are also high priorities for European Supervisory Authorities who expect accurate and complete information.

The challenges of effectively establishing and then maintaining these repositories make them a critical focus for financial institutions to review and refine. However, institutions should ensure that these enhancements do not lead to an expansion of manual processes or a superfluous increase in headcount. Factors such as ongoing third-party contractual renegotiations and amendments, significant technical data and template format requirements, as well as the normal advancement of a bank's ICT assets, will require financial institutions to embed control and automative processes that continually monitor and maintain these registries post go-live as part of an institution's operational resilience operating model and risk capabilities.

> *"However, institutions should ensure that these enhancements do not lead to an expansion of manual processes or a superfluous increase in headcount."*

3 Repaper Existing Vendor Contracts

DORA places significant emphasis on the inclusion of prescribed contractual provisions related to contracts with third-party ICT service providers. In addition to the formalisation of routine contract components, such as service level agreements, data storage location information, and explicit termination clauses - which apply to all providers - contracts with providers of services supporting critical or important functions are subject to enhanced requirements. These include implementing contingency plans, following appropriate security measures, and cooperation with testing programs.

The ECB identified the alignment of contracts with DORA requirements as a key focus in its supervisory priorities for 2025-2027, noting that 10% of the contracts underlying critical or important services at banks analysed in the 2024 SREP were not compliant.[3] Due to the complexity and importance of the aforementioned contracts, the non-compliance rate for contracts related to non-critical services is likely much higher.

Financial institutions should have in place a contract repository that provides an accurate and complete view of DORA-compliant contracts. Any gaps must be identified and prioritised for amendment. However, this has been complicated in the past by difficulties related to co-ordinating with potentially dozens of small to medium-sized vendors who often lack dedicated compliance contacts, as well as by large third-party service providers who may be reluctant to enact contract changes at the request of their customer. Institutions will need to balance managing the risks of non-adherence with the cost of substituting these services.

Reassessing DORA with Monocle

A critical first step in moving from minimum viable solutions to strategically aligned DORA compliance in 2025 is the reassessment of existing efforts and the analysis of the gap between current and future compliance levels.

Monocle's DORA Questionnaire Assessment Tool aims to achieve this by providing a full compliance overview through a set of over 200 targeted questions related to regulatory compliance. The tool aims to provide a pragmatic and comprehensive approach to understanding DORA maturity while exposing gaps and deficiencies. By having identified all the deliverables required by the act and its supporting standards and created a series of simple and direct questions, the tool provides clarity to the exact changes needed to achieve compliance.

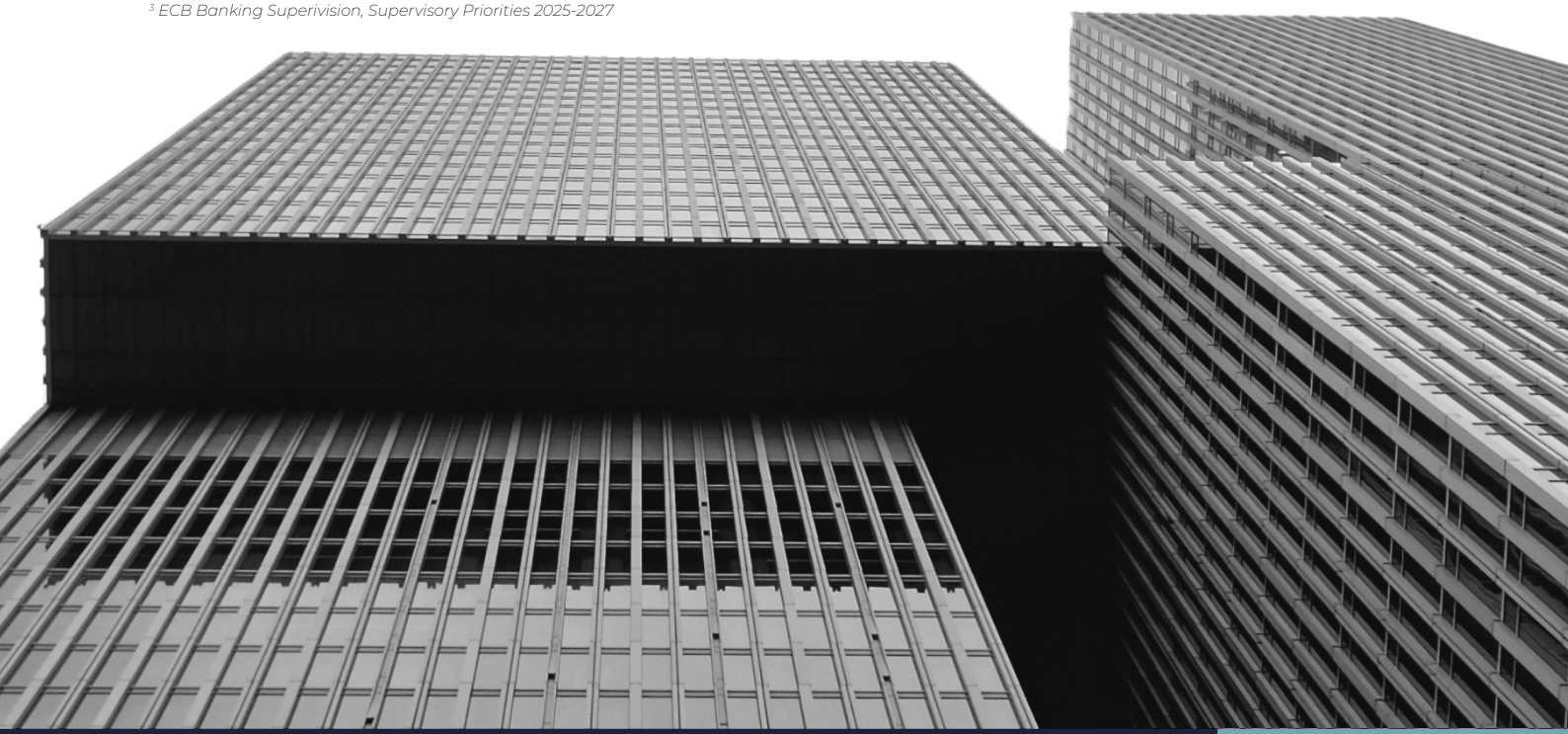
The deliverables are mapped to specific articles and clauses in the legislation, and fall into the following broad categories:

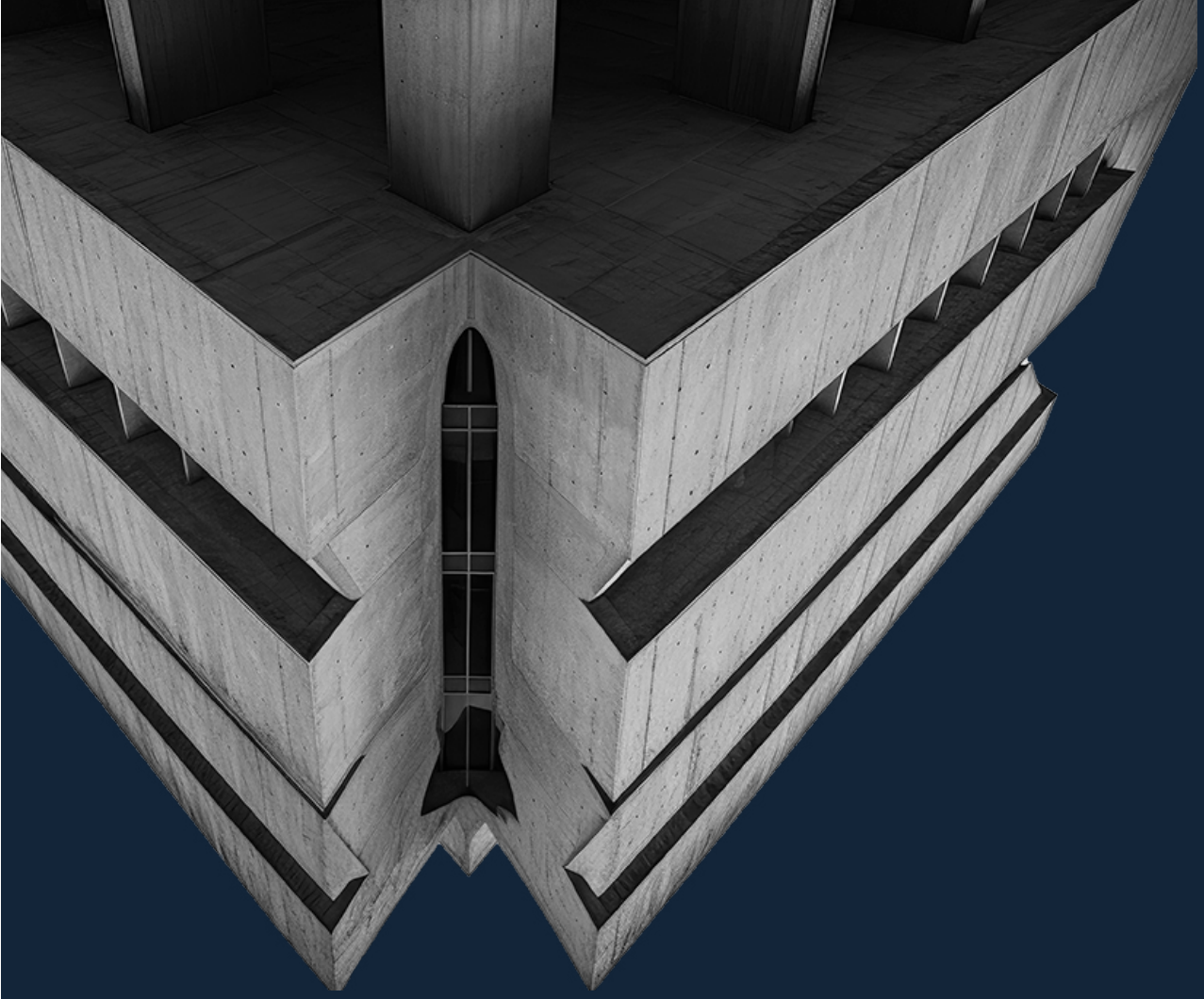
- **Governance roles and functions**
- **Policies, plans, and programmes**
- **Processes and systems**
- **Assessments and reports**

Monocle has over 20 years of specialised expertise and experience in implementing large-scale regulatory and risk projects across major financial institutions. With extensive experience in Basel IV and BCBS 239 implementation, resolution planning, as well as the LIBOR Transition, Monocle has a deep understanding of IT and data governance, operational risk, operational resilience and contract repapering.

Our cross-functional capability to assist our clients with both technical finance, risk and data requirements, while effectively managing large regulatory programmes, enables us to effectively assist our clients with compliance projects covering the broad scope of DORA and add value to our clients' DORA compliance journeys.

[1] *De Nederlandsche Bank, DORA: January 17, 2025 is approaching faster than you think*
[2] *S&P Global, Preparing for DORA Compliance: A Guide for Organisations*
[3] *ECB Banking Superivision, Supervisory Priorities 2025-2027*





MONOCLE

We manifest *change*

Johannesburg

8th Floor, The MARC Tower 1
129 Rivonia Road, Sandton,
Johannesburg, 2196

info.za@monoclesolutions.com

+27 (0) 11 263 5600

Cape Town

301 New Cumberland
163 Beach Rd Mouille Point
Cape Town, 8005

info.za@monoclesolutions.com

+27 (0) 82 952 1415

London

1 Royal Exchange
EC3V 3DG
London, England

info.uk@monoclesolutions.com

+44 (0) 2030 022 514

Amsterdam

Office 136, Gustav Mahlerplein 2,
1082 MA, Amsterdam,
Netherlands

info.nl@monoclesolutions.com

+31 (0) 2 02 256 182

www.monoclesolutions.com