

How DORA Can Drive Business Value Through Data

Beyond Compliance: A Practitioner's Perspective on Operational Resilience in Financial Services

Giovanni Leonardi

March 2024



Contents

1. Executive Summary

3

2. 1. The Problem Nobody Wants to Name

3

3. 2. Why It Is Harder Than It Looks: Three Structural Reasons

4

3.1 2.1 The Five Pillars Are Not Independent

4

3.2 2.2 Third-Party Risk Has a Data Problem

4

3.3 2.3 Legacy Systems Are a Data Governance Problem

4

4. 3. What Good Looks Like: The Three-Level Fix

5

4.1 3.1 The Governance Level: Define Accountability Before Architecture

5

4.2 3.2 The Data and Measurement Level: Build for Regulatory Use from the Start

5

4.3 3.3 The People and Culture Level: Make Compliance Everyone's Problem

5

5. 4. The Regulatory Complication

6

6. Conclusion: The Question Worth Asking

6

How DORA Can Drive Business Value Through Data

Transformation · No. 308

Originally written March 2024 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

1. Executive Summary

The Digital Operational Resilience Act (DORA) presents financial institutions with a defining moment. For most, the instinct is to treat it as a compliance exercise — a set of obligations to be met, boxes to be ticked, and evidence to be filed with the regulator. This paper argues that instinct is both understandable and strategically costly.

Institutions that approach DORA as a compliance minimum will spend significantly, build point solutions, and emerge with a defensible regulatory position and little else. Institutions that approach it as a data governance transformation will spend similarly, build reusable infrastructure, and emerge with operational capabilities they did not previously have. The difference is not in the investment — it is in the framing.

This paper sets out that argument in practical terms: what DORA actually requires at the data level, why those requirements are harder than they first appear, and what a value-generating approach to compliance looks like in practice.

2.1. The Problem Nobody Wants to Name

There is a question that sits beneath most DORA compliance programmes that no one is asking directly: do we actually know where our critical data is, what state it is in, and who is responsible for it?

The uncomfortable answer, for the majority of financial institutions, is no. Not completely. Not consistently. Not in the way DORA requires.

This is not a technology problem. Most large institutions have invested heavily in data infrastructure over the past decade. The problem is governance — the policies, accountabilities, and controls that determine how data is defined, managed, and assured across the organisation. DORA does not introduce new technology requirements so much as it exposes pre-existing governance gaps that institutions have managed around rather than resolved.

The pattern that recurs across regulated environments is consistent: data exists in multiple systems with no single authoritative source; ownership is claimed but not exercised; quality is assumed but not measured; and lineage — the ability to trace data from origin to regulatory report — is reconstructed after the fact rather than maintained in real time.

DORA makes that pattern untenable. Not because regulators will immediately detect it, but because the incident reporting and resilience testing requirements will expose it

under pressure — precisely when the institution can least afford to be exposed.

3.2. Why It Is Harder Than It Looks: Three Structural Reasons

3.1 2.1 The Five Pillars Are Not Independent

DORA's framework is typically described as five pillars: ICT risk management, incident reporting, operational resilience testing, third-party risk management, and data governance and reporting. Most compliance programmes are structured along those same lines — a workstream for each pillar, a lead for each workstream, a steering group above them.

The problem is that the pillars are not independent. Effective ICT risk management depends on accurate, complete, and timely data. Incident reporting requires that data to be available in a structured form at the moment of need — not assembled retrospectively. Resilience testing is only meaningful if the data used to design the tests reflects the actual state of the estate, not a documented version of it that was accurate eighteen months ago.

Compliance programmes that treat the pillars independently will build five defensible workstreams and miss the integration that makes them work. Data governance is not one of five pillars. It is the foundation on which the other four rest.

3.2 2.2 Third-Party Risk Has a Data Problem

Financial institutions' reliance on third-party ICT providers is well understood. What is less well understood is the data dimension of that reliance. DORA requires institutions to monitor third-party providers continuously — not just at contract renewal. That continuous monitoring requires data: performance data, incident data, concentration risk data, contractual compliance data.

Most institutions do not have systematic processes for collecting and maintaining that data. They have contracts. They have questionnaires. They have periodic review meetings. They do not have the data infrastructure to demonstrate continuous monitoring at the level DORA envisages.

Building that infrastructure is not straightforward. Third parties are not obligated to provide data in formats that are convenient for their clients' regulatory reporting pipelines. Standardisation requires negotiation, which requires leverage, which requires a procurement model that most institutions have not yet built.

3.3 2.3 Legacy Systems Are a Data Governance Problem

The third structural challenge is the one most frequently acknowledged and least frequently resolved: legacy technology. Most large financial institutions operate on core systems that were not designed for the data transparency DORA requires. These systems hold critical operational data in formats that are difficult to extract, difficult to reconcile with other systems, and difficult to subject to automated quality controls.

The standard response — build an extract layer, normalise the data, load it into a governance platform — is technically viable and operationally complex. It creates new dependencies, new failure modes, and new questions about which version of the data is authoritative when the extract and the source diverge.

4.3. What Good Looks Like: The Three-Level Fix

4.1 3.1 The Governance Level: Define Accountability Before Architecture

The most common mistake in data governance programmes is to begin with the technology. A new platform is selected, a data catalogue is deployed, a lineage tool is implemented — and twelve months later, the platform is populated with inconsistent metadata, the catalogue has not been maintained, and the lineage tool reflects the documented architecture rather than the actual one.

The reason is not the technology. It is the absence of clear, exercised accountability for data quality at the source. Every critical data element needs an owner — not a system owner, but a business owner who is accountable for the accuracy, completeness, and timeliness of that element and who has the authority and the incentive to enforce standards.

Building that accountability structure is a governance design problem, not a technology problem. It requires decisions about organisational design, role definitions, performance frameworks, and escalation paths. It should be resolved before any technology is selected.

4.2 3.2 The Data and Measurement Level: Build for Regulatory Use from the Start

The second level is data architecture. The principle here is straightforward: design data pipelines for regulatory use from the outset, not as a retrofit. This means defining the regulatory reporting requirements first, working backwards to the data elements required to meet them, and building collection, quality, and lineage controls into the pipeline design rather than adding them later.

In practice, this requires close collaboration between the regulatory reporting function, the data architecture team, and the business lines that own the source data. That collaboration is rarely natural — the functions have different vocabularies, different incentives, and different timelines. Creating the conditions for it to happen consistently is a programme management challenge as much as a technical one.

The measurable outputs of this level are: a complete critical data element inventory, defined quality thresholds for each element, automated quality monitoring in production, and documented lineage from source to regulatory report that can be demonstrated to the regulator on demand.

4.3 3.3 The People and Culture Level: Make Compliance Everyone's Problem

The final level is the most frequently underestimated. Data governance fails not because the policies are wrong or the technology is inadequate, but because the people who generate, handle, and consume data do not treat quality as their responsibility.

In most financial institutions, data quality is treated as someone else's problem — specifically, the data team's problem. Business users generate data, systems capture it, and the data team is expected to find and fix quality issues before they reach the regulator. That model does not scale to DORA's requirements, and it creates a structural dependency that is both expensive and fragile.

The alternative is a model in which data quality accountability is embedded in the business — where the person who originates a data element is accountable for its accuracy, where quality metrics are visible to business managers, and where remediation of quality failures is treated as an operational priority rather than a data team backlog item.

Building that culture requires sustained leadership attention, visible consequences for quality failures, and recognition for quality excellence. It is a change management programme as much as a data governance one.

5. 4. The Regulatory Complication

DORA does not exist in isolation. Financial institutions are simultaneously managing compliance with GDPR, MiFID II, Basel III, PSD2, and Solvency II, among others. Each framework has its own data requirements, its own reporting timelines, and its own regulatory audience.

The temptation — and the trap — is to build separate compliance infrastructure for each framework. The result is a proliferation of data pipelines, governance controls, and reporting processes that overlap, conflict, and consume disproportionate resource to maintain.

The institutions that manage this complexity most effectively are those that invest in a unified data governance layer that serves multiple regulatory frameworks simultaneously. The data elements required by DORA overlap significantly with those required by other frameworks. The quality controls that support DORA incident reporting are the same controls that support MiFID II transaction reporting. The lineage infrastructure that demonstrates DORA compliance is the same infrastructure that supports GDPR data subject access requests.

Building that unified layer requires a higher upfront investment and a more complex programme design. It returns a lower ongoing cost of compliance and a significantly more resilient regulatory position.

6. Conclusion: The Question Worth Asking

Every financial institution subject to DORA will spend money on compliance. The question is not whether to invest but what to invest in. A compliance-minimum approach will produce a defensible regulatory position. A governance-transformation approach will produce that position plus operational capabilities — better data visibility, faster incident response, more reliable third-party oversight, and a foundation for future regulatory

requirements that is already in place.

The choice between those outcomes is not made at the point of regulatory deadline. It is made at programme initiation, in the framing decisions that determine what the programme is actually trying to achieve.

The question every leadership team should be asking now is not: are we compliant? It is: are we building something that will still be worth having when the next regulation arrives?