NETBRAIN TECHNOLOGIES

Digital Operational Resilience and Network Operations

A practical interpretation of DORA using NetBrain

Contents

Executive summary ... 3

Why DORA exists ... 4

The five DORA pillars through an operational lens ... 4

Where network operations typically break down ... 4

NetBrain role in a DORA-aligned operating model ... 5

DORA Operational Mapping ... 5

- 5.1 ICT risk management, governance and operational control ... 5
- 5.2 ICT incident reporting ... 5
- 5.3 Digital operational resilience testing ... 6
- 5.4 ICT third-party risk management ... 7
- 5.5 Information sharing ... 7

What NetBrain Does Not Replace ... 8

NetBrain posture as an ICT third-party supplier ... 8

Practical Takeaway for Regulated Organisations ... 9

Conclusion ... 9

Positioning statement ... 9

NetBrain supports DORA by enabling governed, repeatable and auditable network operations across on-prem and cloud environments.

Executive summary

The Digital Operational Resilience Act (DORA) formalises a reality most financial institutions already understand: ICT failures are no longer isolated technical issues; they are systemic operational risks.

While DORA spans governance, testing, incident reporting, third-party oversight and information sharing, many of the most visible failures originate in day-to-day network operations. Manual troubleshooting, undocumented changes, inconsistent diagnostics, and limited visibility into hybrid and outsourced infrastructure all increase the likelihood, duration and impact of incidents.

This paper examines DORA through an operational lens, focusing on where network operations directly influence regulatory outcomes. It explains how operational automation, standardisation and evidence generation to reduce risk and improve regulatory confidence.

NetBrain is positioned as an operational enablement platform. It does not replace governance, GRC tooling, or regulatory reporting systems. Instead, it helps organisations execute network operations in a controlled, repeatable and auditable way that aligns with DORA expectations.

Why DORA exists

DORA exists because operational failures in ICT environments have repeatedly caused customer harm, market disruption and supervisory concern.

Regulators have observed that:

- ICT incidents are often detected late
- Root cause analysis is inconsistent or incomplete
- Operational actions during incidents are poorly documented
- Outsourced and cloud environments increase dependency risk
- Evidence provided during supervisory review is fragmented or retrospective

In many cases, the issue is not a lack of policy or intent. It is the gap between documented process and actual operational behaviour under pressure.

DORA addresses this gap by requiring organisations to demonstrate:

- Continuous ICT risk management
- Structured incident handling and reporting
- Repeatable resilience testing
- Oversight of third-party ICT dependencies
- Clear governance and accountability
- Evidence that controls operate in practice

The five DORA pillars through an operational lens

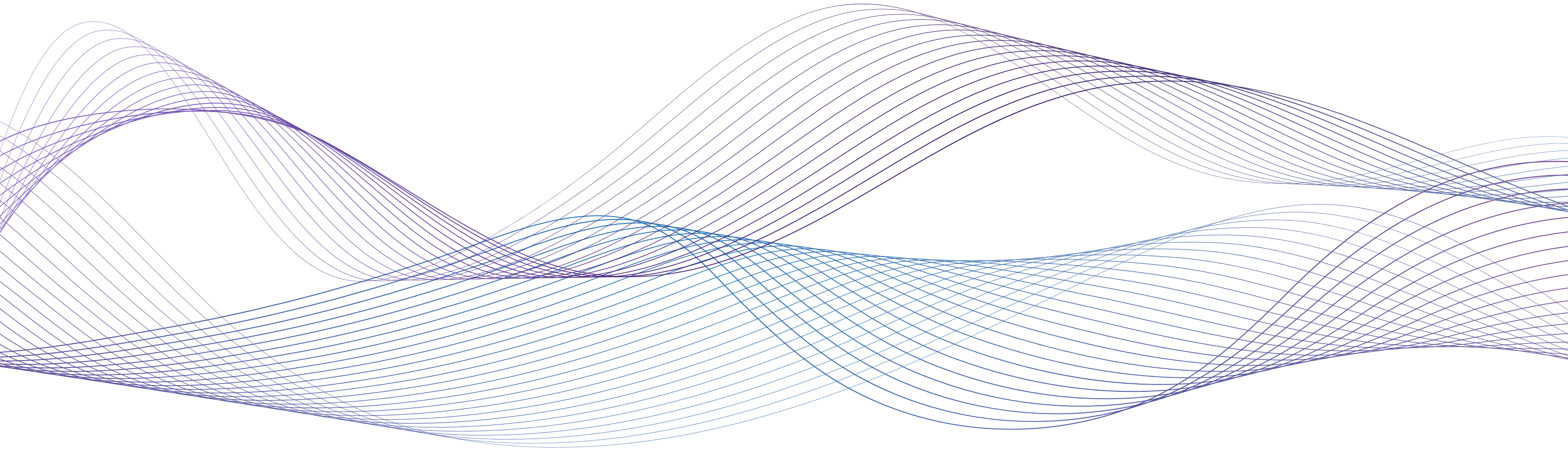
DORA is commonly interpreted through five practical operational pillars:

1. ICT risk management, including governance and operational control
2. ICT-related incident reporting
3. Digital operational resilience testing
4. ICT third-party risk management
5. Information sharing

While these pillars are described separately, they are tightly interconnected in practice. Governance and oversight should not be treated as a disconnected activity. They sit inside ICT risk management as the mechanism that defines accountability, authority, approval, control operation and evidence expectations.

Weakness in one area typically cascades into others. For example:

- Weak governance allows operational actions to occur without clear authority
- Poor risk management increases incident frequency
- Slow detection delays reporting
- Inconsistent testing weakens supervisory confidence
- Third-party blind spots amplify impact
- Weak evidence undermines regulatory trust
- Network operations sit underneath all five pillars.



Where network operations typically break down

Across regulated environments, common operational failure patterns emerge:

- Troubleshooting is manual and engineer-dependent
- Diagnostics vary by individual experience
- Changes are executed under pressure with limited validation
- Evidence is reconstructed after the incident
- Cloud and third-party infrastructure lack equivalent visibility
- Operational knowledge is tribal rather than institutional

These issues are not usually caused by negligence. They arise from scale, complexity, and reliance on human judgement during high-stress events.

DORA raises the bar by expecting organisations to control these variables.

NetBrain role in a DORA-aligned operating model

NetBrain supports DORA by addressing two core operational challenges:

1. Reducing operational risk
2. Producing defensible operational evidence

NetBrain does this by turning network operations into governed, repeatable workflows rather than ad-hoc activities.

NetBrain is the only platform independently validated against Gartner's BRITE framework for Agentic NetOps, which addresses Boundary, Reasoning, Integration, Trust and Explainability. The AI capability is assisted, not autonomous. It surfaces root cause analysis from the live network state and the diagnostic outputs, while the engineer remains in control of the change. That posture matters under DORA, where the management body remains accountable for the operation of ICT risk controls and the supervisory framework expects explainable, auditable behaviour from any AI used in critical functions.

NetBrain is not a compliance platform as it does not replace legal interpretation, regulatory reporting, or secure crisis communications. Its role is to improve how network operations are executed and how evidence of that execution is gained within the environment.

DORA Operational Mapping

5.1 ICT risk management, governance and operational control.

DORA requires financial entities to manage ICT risk through a governed, controlled and accountable operating model. This includes continuous identification, protection, detection, response and recovery across ICT systems, supported by clear responsibility, approval discipline and evidence that controls operate in practice.

From a network operations perspective, ICT risk management is not only a policy activity. It is the ability to prove that the network is being operated, changed, diagnosed and restored in a controlled way.

Articles 5 and 6 of DORA place responsibility for the ICT risk management framework with the management body and require it to be documented, reviewed at least annually, and demonstrably effective. Commission Delegated Regulation (EU) 2024/1774, the RTS on ICT risk management tools, methods, processes and policies, sets out what that framework looks like in practice, including the requirements for ICT operations, asset management, network security, change management and vulnerability handling. Article 8 goes further. It requires identification of all ICT assets, including remote sites, network resources and hardware equipment. Inventories must be maintained and updated periodically and on every major change. Configurations, links and interdependencies must be mapped for those assets considered critical. Article 8(2) separately requires continuous identification of all sources of ICT risk across the ICT estate. For network estates that span on-prem and cloud, these obligations cannot be demonstrated by policy alone. They require a live operational picture that stays current as the network changes.

NetBrain addresses this through a real-time digital twin of the network. The twin is continuously updated from the live environment, not from periodic snapshots, so asset inventory, configuration state and dependency maps reflect the network as it is at the moment of diagnosis or change, rather than as it was at the last audit cycle.

NetBrain supports this in the following ways:

- Continuously validating network state using automation and network intents
- Using Deep Diagnosis (Driven by Agentic AI) to iteratively identify abnormal conditions and likely root cause
- Applying runbooks to standardise operational checks and responses
- Extending visibility across on-prem and public cloud environments
- Controlling access to automation and AI capabilities through explicit privileges
- Enforcing governed remediation workflows through Intents and Change Management
- Supporting approval and pre-approval for automated changes
- Maintaining audit trails of actions and changes linked to users
- Linking ITSM records to executed diagnostics and remediation
- Preserving operational artefacts with version history

Operational impact:

- Reduced reliance on manual troubleshooting
- Earlier detection of network anomalies
- Fewer undocumented operational actions
- Clearer accountability for operational decisions
- Traceable decision-making before remediation
- Reduced operational risk during change and recovery
- Stronger evidence that ICT risk controls operate in practice

In practice, this is the kind of controlled execution DORA expects. RBC, a major global bank, uses NetBrain to run credential audit and rotation workflows at a 99.97% time reduction against the manual baseline, with a 100% change success rate across the estate. The outcome is not speed alone. It is governed, attributable, evidenced change activity at scale, which is exactly what a supervisor wants to see when testing whether ICT risk controls operate in practice.

NetBrain does not replace enterprise risk ownership, board accountability, GRC tooling, legal interpretation or compliance governance. Its role is to strengthen the operational execution layer by making network activity controlled, repeatable, attributable and evidenced.

5.2 ICT incident reporting

Articles 17 to 23 of DORA require a structured ICT incident management process with clear roles, timelines and evidence. Commission Delegated Regulation (EU) 2024/1772 sets the classification criteria and materiality thresholds for major incidents and significant cyber threats. Commission Delegated Regulation (EU) 2025/301 and the accompanying Implementing Regulation (EU) 2025/302 set the operational clock and the reporting templates. The initial notification to the competent authority is due within 4 hours of classifying an incident as major, and in any case within 24 hours of becoming aware of it. An intermediate report follows within 72 hours of the initial notification, and a final report no later than one month after submission of the intermediate report, or the latest updated intermediate report where one has been issued. Each stage requires structured facts, not narrative.

The 4-hour window starts from the moment the incident is classified. Anything that shortens triage, diagnosis and evidence capture directly protects the reporting clock and the quality of what reaches the regulator.

NetBrain supports incident handling in the following way:

- Triggering automated diagnosis from ITSM
- Capturing diagnostic evidence as the incident unfolds
- Producing transparent root cause analysis
- Linking incidents, diagnostics and actions taken
- Exporting structured artefacts for post-incident reporting

NetBrain accelerates technical investigation and evidence capture. It does not replace formal regulatory reporting channels or secure incident communications.

5.3 Digital operational resilience testing

Article 25 of DORA requires regular, repeatable testing of ICT resilience across the estate. Article 26 introduces a separate regime, threat-led penetration testing, for financial entities identified by their competent authority based on impact, financial stability and ICT risk profile considerations. The detailed criteria and methodology are set out in Commission Delegated Regulation (EU) 2025/1190. The two regimes sit alongside each other and serve different purposes. NetBrain supports Article 25 testing as part of day-to-day operational validation. It is not a threat-led penetration testing platform and does not replace a qualified red team under the Article 26 regime.

NetBrain supports testing by:

- Using runbooks as repeatable test workflows
- Allowing scheduled and ad-hoc execution of validation checks
- Providing consistent outputs and execution logs
- Extending testing logic into cloud and API-driven environments
- Reducing dependency on individual engineers during tests

Operational impact:

- Improved test consistency
- Clear evidence of ongoing testing
- Faster identification of weaknesses

5.4 ICT third-party risk management

Article 28 of DORA places third-party risk management at the centre of ICT oversight, with policy requirements specified in Commission Delegated Regulation (EU) 2024/1773 and detailed expectations for subcontracting in Commission Delegated Regulation (EU) 2025/532. Article 28 also introduces the Register of Information, the single inventory of all contractual arrangements with ICT third-party service providers, which financial entities must maintain and submit to competent authorities. Commission Implementing Regulation (EU) 2024/2956 specifies the templates and data points for that submission. The first submission round in April 2025 exposed widespread data quality gaps across the sector, including incomplete records, missing contract identifiers and legal entity identifiers, inconsistent classification of services against the ESA taxonomy, and gaps in dependency information between internal systems and external providers. NetBrain does not produce the Register of Information. It produces the underlying operational evidence that feeds it, specifically the interconnection and dependency data that ties ICT assets to the services and providers they depend on.

NetBrain supports operational oversight by:

- Providing visibility into third-party connected networks
- Monitoring hybrid and cloud environments alongside on-prem
- Correlating incidents across internal and external domains
- Producing evidence of continuous monitoring activity

NetBrain supports monitoring and audit evidence. It does not author contracts or manage regulatory notifications.

5.5 Information sharing

DORA encourages structured information sharing, internally and optionally externally.

NetBrain supports internal sharing by:

- Producing standardised diagnostic artefacts
- Exporting maps, runbook outputs and summaries
- Converting technical outputs into readable summaries for non-network stakeholders

NetBrain does not provide secure external sharing channels. These remain separate controls.

What NetBrain Does Not Replace

For clarity and regulatory safety, NetBrain does not replace:

- GRC platforms
- Regulatory reporting systems
- Secure crisis communications tools
- Legal or compliance advisory functions

NetBrain complements these systems by improving the quality, speed and consistency of operational execution and evidence.

NetBrain posture as an ICT third-party supplier

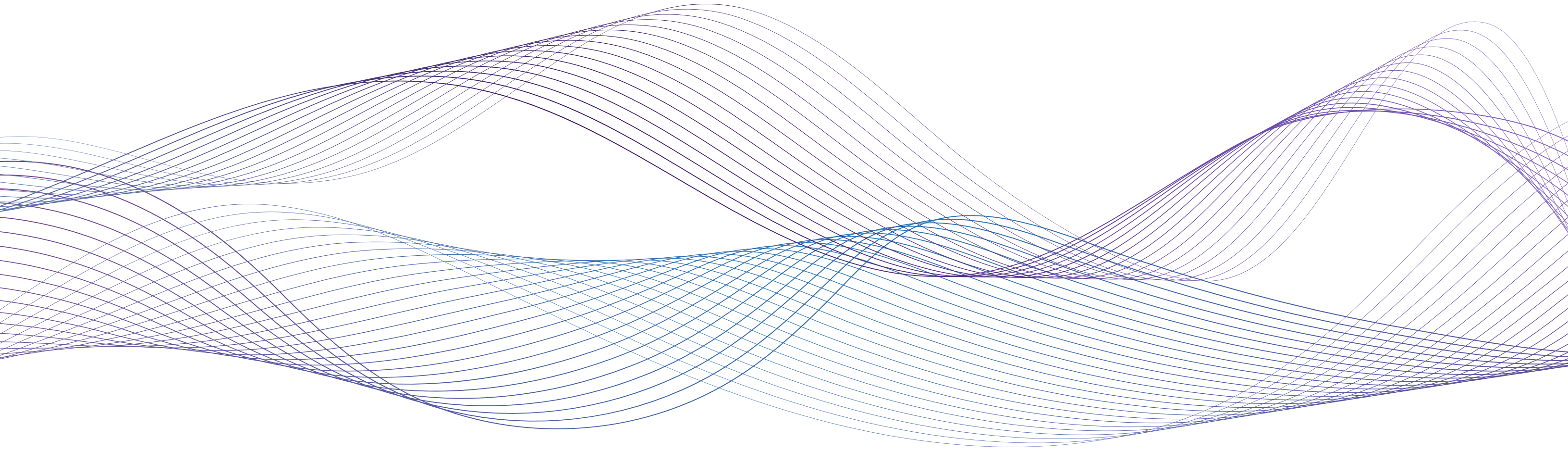
DORA does not stop at the financial entity. Article 30 requires specific contractual provisions in every arrangement with an ICT third-party service provider, including audit rights, sub-processor disclosure, incident cooperation aligned to the reporting regime in Articles 17 to 23, service level commitments and documented exit arrangements. Enhanced provisions apply where the ICT service supports a critical or important function.

When NetBrain is deployed into a DORA-regulated entity, NetBrain is itself an ICT third-party service provider in scope of these obligations. NetBrain provides, or is prepared to provide, the information and cooperation that regulated customers need in order to satisfy Article 30:

- Up-to-date sub-processor and data handling information on request
- Incident communication timelines that align with customer reporting obligations
- Audit evidence and access rights in line with the contract
- Exit and data portability support consistent with contractual exit arrangements
- Cooperation with customer-led testing and oversight activity where required

Regulated customers typically request additional information during supplier due diligence, covering hosting and data residency, security certifications, NetBrain's own business continuity arrangements, and integration with existing operational tooling. NetBrain provides this information on request under appropriate confidentiality terms. Common integration points include IT service management platforms such as ServiceNow, security information and event management systems, configuration management databases and change management workflows.

Designation of an ICT third-party service provider as critical under Article 31 is a supervisory determination made by the European Supervisory Authorities. NetBrain will cooperate with any oversight activity that arises from that framework.



NetBrain complements these systems by improving the quality, speed and consistency of operational execution and evidence.

Practical Takeaway for Regulated Organisations

Organisations that align network operations to DORA principles experience:

- Faster and safer incident response
- Reduced dependency on individual engineers
- Stronger audit readiness
- More consistent regulatory interactions
- Improved confidence in outsourced and cloud environments

DORA compliance is not achieved through policy alone. It is demonstrated through operational behaviour.

Conclusion

DORA raises expectations around how ICT operations are managed, evidenced and governed. Network operations are central to meeting these expectations.

NetBrain supports DORA by turning network operations into controlled, repeatable and auditable workflows. It reduces operational risk and improves evidence quality without replacing existing governance or compliance systems.