JupiterOne

DIGITAL OPERATIONAL RESILIENCE ACT

DORA Is Here. Most Organizations Aren't Ready.

Operational resilience requires real-time visibility. Most financial firms have yet to achieve it.

THE COMPLIANCE GAP

DORA became law in late 2023 and enforcement began January 17, 2025. More than a year later, compliance gaps remain widespread across the industry.

20%

of financial sector organizations said they were ready for DORA when enforcement began

96%

said their data resilience fell short in 2025

44%

remained noncompliant more than a year after enforcement began

THE FUNDAMENTAL SHIFT

DORA demands continuous resilience, not periodic compliance.

Legacy tools, stale data, and outdated processes cannot deliver the real-time visibility DORA demands.

BEFORE DORA	WITH DORA
Periodic audits	Ongoing monitoring
Spreadsheets held evidence	Continuous, data-driven validation
Risk assessed annually or every few years	ICT risk framework adhered to at all times
Static compliance posture	Requires continuous improvement

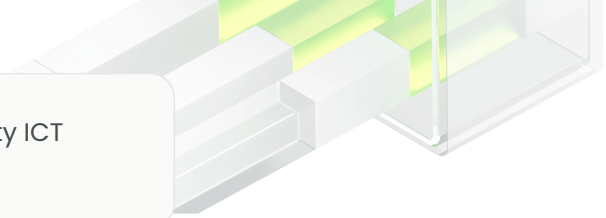
WHERE THE PROBLEM LIES

Disconnected systems. Fragmented data. Limited visibility.

Data silos are major obstacles to DORA compliance — and financial firms are challenged to overcome them.

- GRC tools
- CMDBs
- SIEM
- Cloud resources
- Third-party services

Financial firms struggling with:



46% Maintaining a complete inventory of third-party ICT services and contracts

34% Third-party risk oversight

23% Digital resilience testing and ongoing control validation

WHAT DORA ACTUALLY REQUIRES

A continuous, data-driven view of ICT risk and third-party dependencies.

Manual processes and disconnected data stores cannot deliver what's needed.

Continuous Monitoring

Real-time watch across every ICT asset and third-party integration — no gaps between audit cycles.

Real-Time Asset Visibility

A live, complete inventory of every asset — cloud, SaaS, on-prem — and the relationships between them.

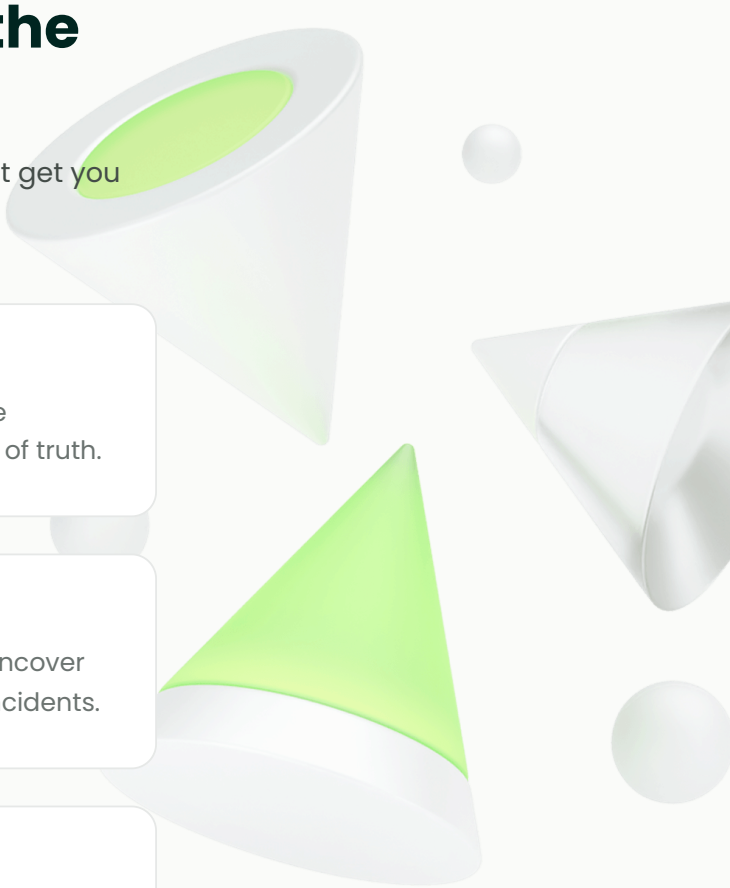
Ongoing Control Validation

Automated, evidence-backed proof that controls are working — not a once-a-year snapshot.

CLOSING THE GAP

Three core capabilities at the heart of DORA readiness.

Point-in-time audits and disconnected data stores cannot get you there.



Unified data

Collect and normalize data from across the entire environment, consolidating it into a single source of truth.

Relationship context

Map the interconnections between all assets to uncover hidden risk and instantly see the blast radius of incidents.

Real-time reporting

All compliance-related asset data in a single, clear, intuitive view — updated continuously, not quarterly.

THE OUTCOME

Go beyond checkbox compliance to real digital operational resilience.

Risks are visible

Understand your environment continuously — not just during audit season.

Dependencies are clear

Every third-party relationship mapped. No surprises in your blast radius.

Response is immediate

Identify and remediate DORA noncompliance the moment it surfaces.

JupiterOne

GRAPH-NATIVE PLATFORM

If you don't understand the relationships between your assets, you can't know your risks.

Built with an **entity-relationship graph** as its foundational data model, JupiterOne's cyber asset graph fully captures every aspect of today's complex cloud- and SaaS-centric environments. The platform supports real-time reporting, making it possible to immediately identify — and remediate — DORA noncompliance.

- 100+ asset classes, 5,000+ unique asset types
- 20,000+ relationship types mapped continuously
- 200+ integrations — cloud, SaaS, on-prem

Download the DORA eBook →

JupiterOne