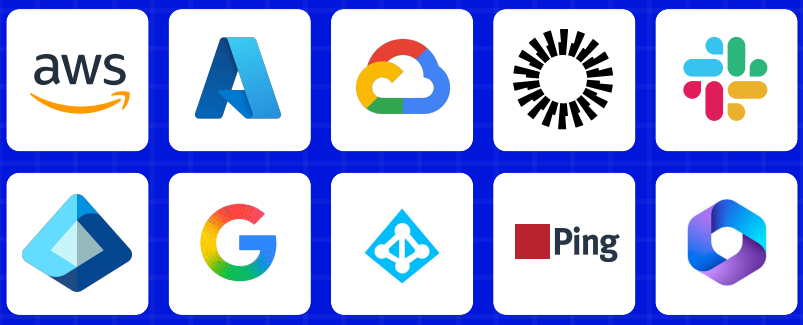
unosecur

WHITEPAPER

DORA, Cloud and Identity

A practical guide for financial entities in EU



100+ more apps & integrations

unosecur.com

sales@unosecur.com

Table of Contents

Executive summary

DORA sets a single EU rulebook for keeping financial services running when ICT fails. It unifies ICT risk, incident reporting, testing, and third-party oversight, and it has become fully applicable from 17 January 2025. In cloud and SaaS estates, identity is the practical control plane.

This paper shows how to see every human and non-human identity, cut standing privilege, detect misuse in real time, and produce regulator-ready evidence. We map key Articles to concrete controls, timelines and metrics, and we show where Unosecur helps you evidence what supervisors expect.

Introduction

The Digital Operational Resilience Act (DORA) is a single EU framework that strengthens ICT governance, testing, incident reporting, third-party oversight, and information-sharing. In cloud-heavy organisations, operational resilience lives in identity and access.

Every user, device and machine identity must be visible, governed and provable.

Chapter I. General provisions (Articles 1-4)

Scope and proportionality

DORA applies across the EU financial sector and embeds proportionality, so controls scale with your size, services and risk profile. Anchor proportionality in the risk appetite approved by the management body, and evidence review cycles.

Chapter II. ICT risk management (Articles 5-16)

Governance, protection and recovery

The management body defines and owns ICT risk governance, approves strategy and budgets, and keeps clear roles, training and reporting. Maintain a documented ICT risk framework with detection, response and recovery, and yearly tests on ICT supporting critical or important functions.

Practical identity controls auditors expect include joiner-mover-leaver flows tied to HR events, time-bound elevation for admin roles, periodic attestation for high-risk entitlements, and monitored break-glass accounts.

Identity in practice

Hybrid estates scatter identity across directories and applications. Unify visibility over human and non-human identities, minimise standing privilege, and monitor elevation paths. This ties prevention, detection and recovery together.

Chapter III. ICT incident management, classification and reporting (Articles 17–23)

From visibility to accountability

Standard processes are required to detect, classify and report major ICT incidents using harmonised templates. Design workflows that can pre-fill the initial notification from identity telemetry, especially for credential theft, token misuse, SSO bypass and privilege escalation.

- Timelines:
- Initial notification within 4 hours of classifying the incident as major, and no later than 24 hours from detection or awareness.
- Intermediate report within 72 hours of the initial notification.
- Final report within one month of the intermediate report.

Chapter IV. Digital operational resilience testing (Articles 24–27)

Validate against identity-based attack paths

Run a risk-based testing programme with independent testers, and test at least yearly all ICT that supports critical or important functions. For entities selected by supervisors, perform Threat-Led Penetration Testing (TLPT) on production against critical functions, at least every three years in general, with clear rules on scope and independence.

Keep the scoping note, rules of engagement, replay and closure evidence ready for inspection. Where mandated, align with TIBER-EU and include purple-teaming during closure.

Chapter V. Managing ICT third-party risk (Articles 28–44)

Oversight in a connected ecosystem

Keep a third-party strategy, a register of ICT services, concentration risk analysis, audit rights, exit plans and access logging in contracts. DORA also creates EU-level oversight of critical ICT third-party providers, with the European Supervisory Authorities acting as Lead Overseers and a formal Oversight Forum.

Expect recommendations, information requests and inspections at the EU level to flow down to your own supervisory dialogue. Monitor machine identities, service accounts and API tokens that traverse provider boundaries.

Chapter VI. Information-sharing arrangements (Article 45)

Share anonymised threat intelligence and common misconfiguration patterns through sector schemes and ISACs. Protect personal data and customer identifiers.

Chapter VII. Competent authorities and professional secrecy (Articles 46–56)

Keep auditable packs for access reviews, TLPT artefacts and incident files. Protect evidence with role-based access and immutable logs. Supervisors expect timely production on request.

Chapter VIII. Delegated acts (Article 57)

The Commission can adopt delegated acts to refine criteria and fees, including for the oversight of critical ICT providers. Build an evidence pipeline that can adapt without re-engineering.

Chapter IX. Transitional and final provisions (Articles 58–64)

Supervisors look for measurable progress, not one-off projects. Track reduction in standing admin roles, orphaned accounts, token-reuse detections, elevation duration, time to revoke compromised credentials, and MTTD/MTTR.

How Unosecur proves resilience under DORA

Identity Fabric

One view of every human and non-human identity across AWS, Azure, GCP, Okta, Google Workspace, Salesforce and more.

Risk score by role, privilege and exposure, then export straight into an evidence pack for supervisors. Supports proportionality under Chapter II.

IAM Ops and IAM Analyzer

Enforce Just-in-Time and Just-Enough-Privilege for admin roles, and continuously surface unused or excessive entitlements. Every elevation and policy change lands in an immutable audit trail.

This directly supports Articles 5–11 on identification, protection, detection, response and recovery, and it makes access decisions auditable end-to-end.

Identity Threat Detection and Response (ITDR)

Watch every access transaction in near real time, correlate anomalies such as token reuse, privilege jumps and SSO bypass, and trigger workflowed responses.

Pre-built incident templates align to DORA's initial, intermediate and final reporting so teams can meet the 4-hour, 72-hour and one-month windows.

Evidence and Reporting

Automate regulator-ready artefacts: elevation logs, attestation outcomes, TLPT closure notes, incident files and improvement metrics. Align outputs with Articles 17–23, 24–27 and 28–44 so evidence maps cleanly to Chapters III–V.

Appendix. quick mapping table

DORA Area	Articles	What Supervisors Expect	Unosecur Control	Evidence Produced
Incident reporting	17-23, RTS/ITS	Initial in 4 hours of classification and no later than 24 hours from detection or awareness; intermediate in 72 hours of initial; final in one month.	ITDR with templated incident files and identity artefacts	Timestamps, identity trail, PDF/CSV exports
Resilience testing	24-27	Yearly tests on ICT for critical or important functions. TLPT at least every three years for selected entities, production scope, and independence.	Identity-aware attack-path scenarios; TLPT-ready exports	Scoping note, replay, findings, remediation closure
Third-party oversight	28-44	Contractual audit rights, logging, exit plan; ESAs Lead Overseer model for critical providers.	Third-party identity monitoring, contract clause checklist	Access logs, provider register, oversight responses

Next 30 days

1. Turn on JIT/JEP for all admin roles in two critical applications.
2. Run a high-risk entitlement attestation and close exceptions.
3. Dry-run the DORA initial notification using last quarter's top identity alert.
4. Draft a TLPT scope focused on your top two identity attack paths.

Conclusion

Resilience now means three simple things: see every identity, cut standing privilege, and prove it on demand. DORA gives the structure, cloud, and identity gives the leverage. Security is serious, life need not be, but your evidence pack should always be immaculate.

Disclaimer

This paper is informational and not legal advice. Confirm interpretations with counsel and your competent authority.

Verification notes (for your records)

- Application date: 17 January 2025.
- Incident reporting timelines: initial 4 hours from classification and within 24 hours of detection or awareness; intermediate 72 hours from initial; final one month from intermediate.
- Yearly testing of ICT supporting critical or important functions, and TLPT at least every three years for selected entities.
- Lead Overseer model for critical ICT third-party providers, EU-level oversight by the ESAs.

Trusted by security leaders

Unosecur's agentless onboarding approach helped us to strategize and streamline our cloud identity security efforts. The proof of value was achieved in no time, helping us to fix existing identity blind spots.

Vijay Muthu
CISO, Rakuten Symphony

Rakuten Symphony

Ready to secure your enterprise identities?

Scan the QR code to get your free identity risk assessment

ISO 27001 Certified · AICPA SOC · GDPR · Cloud Security Alliance Trusted Cloud Provider CSA · HIPAA COMPLIANT

unosecur

Unified identity fabric for modern enterprises