ManageEngine

A quick guide to DORA

Digital Operational Resilience Act
Regulation (EU) 2022/2554

DORA (Regulation (EU) 2022/2554) is a binding EU law enforcing digital operational resilience for financial entities and critical ICT providers across 20+ institution types, and has been in force since January 2025.

Requirement area	Article	Key controls to implement
ICT risk identification & asset management	Art. 8	• Classify all ICT-supported functions, roles and responsibilities • Maintain full inventory of information & ICT assets, including remote sites • Map critical assets and their interdependencies • Identify third-party ICT dependencies for critical functions • Run annual legacy ICT risk assessments • Update inventories after every major infrastructure change
Protection & access controls	Art. 9	• Document information security policy (availability, integrity, confidentiality) • Enforce phishing-resistant MFA (FIDO2, biometric, risk-adaptive) • Implement least-privilege and RBAC • Run periodic access-rights reviews and recertification campaigns • Encrypt data at rest, in use, and in transit per classification • Segment network for instant isolation on cyberattack • Manage ICT changes via documented, risk-based change processes • Maintain patch and software update policies
Threat detection & monitoring	Art. 10	• Deploy mechanisms to detect anomalous activities and network issues • Define multi-layer alert thresholds with automated escalation • Monitor user activity, anomalies, and cyberattacks continuously • Baseline user/entity behaviour (UEBA) to detect deviations • Correlate logs against threat-intel feeds and MITRE ATT&CK rules • Test all detection mechanisms regularly

Incident management & response	Art. 17	• Establish documented ICT incident process (detect → manage → notify) • Log, categorise, and classify incidents by priority and severity • Define early-warning indicators and senior-management escalation paths • Execute containment and recovery playbooks to restore services • Conduct root-cause analysis; document and address findings • Maintain crisis-communication procedures for all stakeholders
Major incident reporting	Art. 19	• Initial report to competent authority within four hours of classification • Intermediate report within 72 hours with full impact assessment • Final report within one month: root-cause analysis and corrective actions • Retain complete incident timeline, evidence, and technique tagging
Backup, recovery & business continuity	Art. 11–12	• Define Recovery Time Objective (RTO) /Recovery Point Objective (RPO) for all functions • Schedule encrypted, segregated backups (AD, M365, cloud identities) • Validate restoration at attribute, object, and full-system level • Test continuity and recovery plans at least annually • Include cyberattack and switchover scenarios in testing • Maintain BIA covering all third-party ICT dependencies
Threat intelligence & information sharing	Art. 13, 45	• Ingest threat-intel feeds (STIX/TAXII, dark-web, curated IOCs) • Automatically correlate indicators against monitored telemetry • Participate in cyberthreat information-sharing arrangements • Conduct post-incident reviews; feed learnings into risk framework
Digital operational resilience testing	Art. 24–26	• Run annual vulnerability assessments and penetration tests on critical systems • Conduct threat-led penetration testing (TLPT) for significant entities • Test detection mechanisms within the resilience-testing programme • Remediate all findings; update testing scope after major changes

Source: https://www.digital-operational-resilience-act.com/DORA_Articles.html

DORA and ManageEngine

DORA and ManageEngineAD360, ManageEngine's IAM solution, and Log360, its unified SIEM with integrated DLP and CASB, help financial entities implement, monitor, and evidence DORA's technical controls across ICT risk management, incident handling, and information sharing. Together, you can implement the controls required under DORA across on-premises, cloud, and hybrid environments.

How can ManageEngine help you implement DORA?

Adaptive MFA

Enforce phishing-resistant FIDO2, biometric, and risk-adaptive MFA across Windows, macOS, Linux, VPN, and enterprise applications, evaluating device, location, and behaviour signals on each access attempt.

Helps with Art. 9(4)(d).

Access governance and certification

Provision identities through the joiner-mover-leaver life cycle, enforce least privilege through RBAC and OU-based delegation, and run scheduled recertification campaigns.

Helps with Art. 8(1) and Art. 9(4)(c).

Real-time security analytics

Collect, normalise, and correlate logs from servers, endpoints, networks, databases, and cloud platforms against 2,000+ MITRE ATT&CK-mapped detection rules in real time.

Helps with Art. 9(1) and Art.

UEBA and anomaly detection

Baseline user and entity behaviour with ML-tuned thresholds and flag deviations such as impossible travel, off-hours access, and lateral-movement patterns.

Helps with Art. 10(1) and Art. 10(3).

File integrity monitoring and DLP

Track creation, modification, and deletion of sensitive files. Classify data and block exfiltration across endpoint, email, and removable media.

Helps with Art. 9(2) and Art. 9(3).

Automated incident response

Execute prebuilt SOAR playbooks to disable accounts, isolate hosts, block IPs, and raise tickets within seconds of an alert firing.

Helps with Art. 11(2) and Art. 17(1).

Threat intelligence

Ingest curated, dark-web, and STIX/TAXII feeds totalling over a billion indicators, and automatically match them against monitored telemetry.

Helps with Art. 13(1) and Art. 45(1).

Backup and restoration

Schedule encrypted, segregated backups for Active Directory, Entra ID, Microsoft 365, and Google Workspace with attribute-level, object-level, and full restoration.

Helps with Art. 12(1) and Art. 12(3).

Incident workbench and reporting

Manage incidents as cases with timeline, evidence, MITRE technique tagging, Zia Insights and GenAI root-cause narratives ready for Article 19 initial, intermediate, and final reports.

Helps with Art. 17(2) and Art. 19(4).

For more information, contact sales@manageengine.com