TECHNICAL BRIEF

Supporting DORA with Cayosoft Guardian and Cayosoft Administrator

Published:
2026

Sponsored by:
Cayosoft

+1 (614) 423-6718

DORA Five Pillars Coverage Overview

DORA Pillar	Regulatory Requirement	Cayosoft Guardian	Cayosoft Administrator
ICT Risk Management	Identify, assess, and reduce ICT risk across critical systems	Continuous detection of identity misconfigurations, privilege abuse, and attack paths across AD, Entra ID, M365, and Intune	Preventative governance through RBAC, delegation, and automation to reduce identity risk before incidents occur
ICT Incident Management, Classification, and Reporting	Detect, classify, and document ICT-related incidents	Real-time detection of identity-based attacks and configuration changes with full event context	Complete audit trail of identity operations and administrative actions
Digital Operational Resilience Testing	Regularly test resilience and recovery capabilities	Automated, isolated identity recovery testing with validation	Supports operational execution and repeatable workflows
Managing ICT Third-Party Risk	Control risks introduced by external providers and dependencies	Monitoring of service accounts, delegated access, and hybrid identity activity	Governance of hybrid, cloud, and third-party identity operations
Information Sharing	Share threat intelligence and resilience insights across stakeholders	Actionable identity threat intelligence and forensic evidence	Reporting aligned to SOC, audit, risk, and compliance teams

Overview

The Digital Operational Resilience Act (DORA) requires organizations to demonstrate that critical ICT services can be governed, monitored, defended, and recovered under adverse conditions. Identity systems such as Active Directory, Entra ID, Microsoft 365, and Intune are central to this requirement because they underpin authentication, authorization, administration, and service availability across the enterprise.

Cayosoft supports DORA by securing the identity control plane through a unified platform approach:

- Cayosoft Administrator delivers preventative governance, access control, and operational enforcement
- Cayosoft Guardian provides continuous monitoring, threat detection, auditability, and identity recovery

Together, these capabilities address all five DORA pillars, not just detection, and extend beyond on premises directories into cloud and endpoint identity dependencies.

Why Identity Is Foundational to DORA

DORA is not a tool-driven regulation. It is an outcome-driven regulation focused on:

- Continuous ICT risk management
- Early detection and classification of incidents
- Proven recoverability of critical services
- Evidence-based audit and reporting
- Ongoing resilience testing

Identity infrastructure directly impacts all of these outcomes. Modern attacks rarely begin with application exploitation. They begin by abusing identity to escalate privileges, establish persistence, disable controls, and delay recovery. If identity fails, all dependent services fail with it.

Cayosoft treats identity as Tier 0 critical infrastructure, not simply an access management function.

Cayosoft Administrator

Identity Governance, Control, and Risk Reduction

Cayosoft Administrator provides the preventative controls required to reduce ICT risk before incidents occur.

Core Capabilities

Centralized Identity Administration

- Unified management of Active Directory, Entra ID, Microsoft 365, and Intune
- Native support for hybrid and cloud-only environments
- Consistent control model across platforms

Role-Based Access and Delegation

- Granular role and rule-based administration
- Enforced least privilege without standing native admin roles
- Segregation of duties aligned to operational reality

Automation and Policy Enforcement

- Automated provisioning, deprovisioning, and access changes
- Reduced manual intervention and configuration drift
- Policy-driven identity operations instead of ad hoc changes

Audit and Reporting

- Full visibility into identity operations
- Evidence to support compliance reviews and internal controls

DORA Impact

Administrator directly supports ICT risk management by reducing the likelihood and blast radius of identity-based incidents, rather than relying on post-incident remediation.

Cayosoft Guardian

Continuous Monitoring, Detection, and Auditability

Cayosoft Guardian provides the detective and corrective controls required by DORA.

Continuous Identity Monitoring

Guardian continuously monitors identity systems for:

- Privilege escalation and role abuse
- Unauthorized configuration changes
- Persistence mechanisms used by attackers
- Configuration drift across AD, Entra ID, M365, and Intune

This enables detection of identity-driven attacks that bypass traditional endpoint and network defenses.

Change Tracking and Incident Evidence

All identity-relevant changes are recorded with full context:

- What changed
- When it changed
- Where it changed
- How it changed

This creates an audit-ready record that supports incident classification, reporting, and regulatory review.

Identity Recovery and Operational Resilience

DORA requires organizations to prove they can recover critical ICT services, not merely state that backups exist.

Guardian Forest Recovery

Guardian Forest Recovery delivers automated, identity-focused recovery:

- Recovery of Active Directory, Entra ID, Microsoft 365, and identity-dependent services
- Clean, isolated recovery environments
- Restoration of identity components without restoring compromised operating systems
- Validation to prevent reintroducing attacker persistence

Key Characteristics

Isolation

Recovery occurs outside the production environment, reducing reinfection risk.

Automation

Manual recovery runbooks are replaced with structured, repeatable workflows.

Integrity Validation

Identity state is validated before production cutover.

This capability directly supports DORA business continuity and resilience requirements.

Digital Operational Resilience Testing

DORA mandates ongoing testing of resilience capabilities.

Cayosoft enables:

- Scheduled, automated identity recovery testing
- Validation of recovery objectives
- Documented outcomes suitable for regulatory evidence

This shifts recovery from a theoretical plan to a continuously validated operational capability.

Managing Third-Party and Cloud Identity Risk

DORA extends accountability to third-party ICT dependencies, including cloud services.

Cayosoft addresses this by:

- Governing service accounts, delegated access, and automation identities
- Monitoring identity activity across hybrid and cloud platforms
- Extending controls into Microsoft 365 and Intune, where modern service dependencies reside

This ensures that cloud identity and endpoint control planes are included in DORA scope.

Technical Summary

Cayosoft delivers full-spectrum identity resilience aligned to DORA:

- Administrator reduces ICT risk through governance, least privilege, and automation
- Guardian detects identity threats, provides audit evidence, and supports incident reporting
- Guardian Forest Recovery proves recoverability through clean, automated identity restoration

By covering governance, detection, recovery, and testing across AD, Entra ID, Microsoft 365, and Intune, Cayosoft addresses all five DORA pillars with a single, unified identity platform.