

DORA: How Specops Helps You Comply

DORA: Quick Summary

What's DORA? The Digital Operational Resilience Act (Regulation EU 2022/2554) is a mandatory EU cybersecurity framework.

What does DORA cover? It focuses on ICT risk management, identity and access control, incident detection and reporting, operational resilience testing, third-party risk management, and cyber threat information sharing.

Who does DORA apply to? Banks, insurers, investment firms, payment and e-money institutions, crypto-asset service providers, and critical ICT third-party service providers operating in or serving the EU financial sector.

Is it the same as NIS2? No. NIS2 applies broadly across critical sectors; DORA is specific to financial services and supersedes NIS2 for in-scope financial entities. Both share goals around cyber resilience, but DORA sets a higher, more prescriptive bar for the financial sector.

Are there fines for non-compliance? Yes. Financial entities can face fines of up to 2% of total annual worldwide turnover, or up to 1% of average daily global turnover. Individuals responsible for compliance failures can face penalties of up to €1 million.

Why Specops for DORA?

DORA Requirement	How Specops Supports Compliance
Password Visibility	Specops Password Auditor (free tool)
DORA Article 8 Identification Financial entities must identify and assess ICT risks, including vulnerabilities tied to user credentials and access rights across their environment.	Runs a read-only scan of your AD environment to surface compromised, blank, stale, and non-expiring passwords. Generates exportable compliance reports.
Compromised Credentials	Specops Password Policy with Breached Password Protection
DORA Article 9(4)(d) Protection and Prevention Financial entities must implement policies and protocols for strong authentication mechanisms, including controls to ensure credentials used to access ICT systems are not compromised or weak.	Most tools only block breached passwords at change or reset. Specops continuously scans your AD and block against our ever-growing database of 6 billion+ compromised passwords.

DORA Requirement	How Specops Supports Compliance
Strong MFA <i>DORA Article 9(4)(d) Protection and Prevention</i> Financial entities must implement policies and protocols for strong authentication mechanisms, particularly for remote access to the network, privileged access, and access to systems supporting critical functions.	<u>Specops Secure Access</u> Add phishing-resistant MFA for Windows logon, RDP and VPN. Includes SSO support for SaaS applications via OIDC and SAML, and integrates with SIEM, SOC, & Analytics platform.
Service Desk Verification <i>DORA Article 9(4)(c) & 9(4)(d) Protection and Prevention</i> Access rights controls and strong authentication must extend to operational processes, including the service desk, where identity verification failures represent a direct ICT risk.	<u>Specops Secure Service Desk</u> Agents verify caller identity via MFA (20+ methods) before any account action. Full audit log of every interaction. Integrates with ITSMs, plus SIEM, SOC, & Analytics platforms.
High Assurance Verification <i>DORA Article 9(4)(c) & 9(4)(d) Protection and Prevention</i> Strong authentication requirements apply to identity verification for access to ICT systems, including high-risk actions such as account recovery and privileged access reinstatement.	<u>Specops Verified ID</u> Scans government-issued ID and carried out a biometric liveness check for highest-assurance verification.
Secure Password Resets <i>DORA Article 9(4)(c) & 9(4)(d) Protection and Prevention</i> Access controls and strong authentication requirements apply throughout the identity lifecycle, including the password reset process, which must not represent a weaker link than primary authentication.	<u>Specops uReset</u> MFA-gated self-service password reset. Users can securely update local cached credentials from any location, device, or browser, whether on or off VPN. Integrates with SIEM, SOC, & Analytics platform.

Contact your Specops account team or visit [here](#) to book a scoping call.

[Book Now](#)