

DORA Operational Resilience Statement

Public statement

27 July 2026

01 What is DORA?

DORA is the EU Digital Operational Resilience Act for the financial sector. It sets requirements for ICT risk management, incident handling, resilience testing, supplier oversight, and governance.

02 Rosslyn's position

Rosslyn is a software provider to clients. DORA regulatory obligations remain with each regulated financial entity, but Rosslyn supports customer assurance through its ISO 27001-aligned controls.

03 Assurance basis

Rosslyn's ISMS is certified to ISO/IEC 27001:2022 for the design and programming of software and the implementation, storage, use, distribution and support of data services, in the UK and International.

Statement of Commitment

Rosslyn maintains an Information Security Management System (ISMS) designed to protect the confidentiality, integrity and availability of information assets, support secure delivery of cloud-based data services, and provide a structured basis for operational resilience. Rosslyn's ISMS operates with documented policies, risk assessment, security controls, incident management, business continuity, supplier governance, monitoring, audit and continual improvement.

Client-facing Assurance scope

- ICT risk is managed through the ISMS, risk assessment and treatment process, information security objectives, and documented controls.
- Security incidents are handled through a Cyber Incident Response Plan covering detection, identification, triage, containment, evidence handling, recovery and post-incident learning.
- Business continuity and disaster recovery arrangements are documented, reviewed and tested, including backup and recovery arrangements for cloud services.
- Secure development practices are embedded into application design, code review, static and dynamic testing, deployment controls and vulnerability response.
- Supplier security is addressed through due diligence, contractual obligations, supplier assessment and ongoing review under Rosslyn's ISMS.

DORA to ISO 27001 alignment

DORA focuses on digital operational resilience for financial entities; ISO/IEC 27001 provides a certifiable management system framework for security governance, risk management and continual improvement.

Rosslyn uses ISO/IEC 27001 as the foundation for many of the controls clients typically assess under DORA supplier due diligence.

DORA theme	What clients need confidence in	ISO 27001 approach
ICT risk management	Technology and cyber risks are identified, assessed, treated and monitored.	Rosslyn maintains an ISO/IEC 27001:2022 ISMS, risk-based security objectives, access controls, encryption, monitoring and supplier obligations.
Incident management and reporting	Security events are detected, classified, escalated and communicated appropriately.	Rosslyn maintains a Cyber Incident Response Plan covering detection, identification, classification, triage, evidence preservation, recovery and post-incident learning.
Business continuity and recovery	Critical services can be maintained or restored following disruption.	Rosslyn maintains a Business Continuity Plan, cloud disaster recovery strategy, backups, defined RTO/RPO approach and regular testing/review.
Resilience testing	Controls are tested through security, continuity and recovery activities.	Rosslyn performs backup recovery testing, BCP/DR exercises, vulnerability management and annual external penetration testing.
Third-party ICT risk	Supplier and subcontractor risks are known, governed and reviewed.	Rosslyn uses supplier due diligence, contractual obligations, supplier risk assessment and supplier service monitoring through its ISMS.
Governance and improvement	Management oversight, audit evidence and lessons learned are maintained.	Rosslyn uses policy ownership, management review, internal audit, corrective actions and continual improvement under ISO 27001.

Important limitation:

This statement is an assurance summary; Rosslyn would not typically fall within the scope of critical or important functions under DORA. This statement does not transfer or replace any DORA obligations held by regulated financial entities, and it should be read with the relevant contract, security schedule, DPA and any customer-specific assurance documentation.

Document control and references

EU Regulation 2022/2554 (DORA)

ISO 27001 certificate, ISMS scope, security/BCP/CIRP/SDLC policies