Compliance Automation

Meeting DORA, SOC 2, and ISO 27001 Requirements

September 2024

45 Pages

Nexora Security Research Team
security@nexora.io

Executive Summary

Regulatory compliance is a critical requirement for modern enterprises. This whitepaper details automated compliance mapping, evidence collection, and continuous monitoring for DORA ICT, SOC 2 Type II, and ISO 27001.

Nexora automates 87% of compliance activities, reducing audit preparation time from months to days.

Continuous compliance monitoring ensures organizations maintain certification status year-round.

1. EU DORA Compliance

1.1 Digital Operational Resilience Act

EU Regulation 2022/2554 requirements:

- ICT risk management framework
- ICT-related incident reporting
- Digital operational resilience testing
- Third-party ICT service provider management
- Information sharing arrangements

1.2 Nexora DORA Controls

Automated compliance implementation:

- Real-time ICT risk assessment
- 72-hour incident reporting automation
- Continuous resilience testing
- Third-party risk monitoring
- Threat intelligence sharing

2. SOC 2 Type II

2.1 Trust Services Criteria
AICPA SOC 2 controls:
• CC6.1: Logical and physical access controls
• CC6.2: Prior to issuing system credentials
• CC6.3: Removes access when appropriate
• CC7.2: System monitoring
• CC7.3: Evaluates security events

2.2 Automated Evidence Collection
Continuous compliance monitoring:
• Access control logs (immutable)
• Credential lifecycle tracking
• Automated access reviews
• Security event correlation
• Audit trail generation

3. ISO 27001:2022

3.1 Information Security Controls
ISO/IEC 27001:2022 Annex A:
• A.9.2: User access management
• A.9.4: System and application access control
• A.12.4: Logging and monitoring
• A.16.1: Information security incident management

3.2 Nexora ISO Controls
Automated control implementation:
• Centralized access management
• Continuous access monitoring
• Real-time log analysis
• Automated incident response
• Compliance reporting dashboard

4. References

[1] EU DORA Regulation (EU) 2022/2554, European Union, 2022
[2] AICPA SOC 2 Trust Services Criteria, AICPA, 2023
[3] ISO/IEC 27001:2022 Information Security, ISO, 2022