NIST & DORA – A Side-by-side comparison

Carlos Alves

November 2024

INTRODUCTION

Here below a synopsis of NIST and DORA

	NIST	DORA (EU Digital Operational Resilience Act)
Description	U.S. government agency that develops standards for technology, cybersecurity, and software.	EU regulation designed to enhance digital operational resilience in the financial sector.
Used For	Enhancing security, ensuring compliance, and improving system reliability.	Regulating ICT risk management and resilience for financial entities within the EU.
Where It Should Be Applied	Organizations requiring strong cybersecurity and compliance (e.g., government, finance, healthcare).	Financial institutions, ICT service providers, and critical financial infrastructures in the EU.

Detailed Comparison Table

	NIST	DORA (EU Digital Operational Resilience Act)
Focus	Security, reliability, compliance, and standards for technology systems.	Digital operational resilience and ICT risk management in the financial sector.
Primary Goal	To establish secure, resilient, and reliable systems.	To ensure the EU financial sector can withstand and recover from ICT-related disruptions.
Key Frameworks/Models	NIST Cybersecurity Framework (CSF), Secure Software Development Framework (SSDF), SP 800-series.	Regulatory framework with specific requirements for ICT risk management and operational resilience.
Metrics	Risk, resilience, and security performance indicators.	Mandatory compliance measures for ICT risk management, testing, incident reporting, and governance.
Approach	Voluntary adoption of guidelines unless mandated by contracts or regulations.	Mandatory compliance for financial entities operating within the EU, with penalties for non-compliance.
Culture Emphasis	Focuses primarily on technical standards and frameworks, with some attention to organizational culture.	Emphasizes governance, risk management, and structured accountability for resilience.

	NIST	DORA (EU Digital Operational Resilience Act)
Security Integration	Promotes integrating security in software development lifecycle (e.g., DevSecOps).	Mandates robust ICT risk management, resilience testing, and third-party risk monitoring.
Incident Recovery	Provides guidelines for resilience and recovery after cybersecurity incidents.	Requires mandatory reporting and recovery protocols for ICT-related incidents and disruptions.
Regulatory Compliance	Can become mandatory when tied to specific government contracts or industry standards.	Fully mandatory regulation for financial entities in the EU, with specific compliance deadlines (by 2025).
Automation	Encourages automation to enhance security testing and monitoring.	Encourages automated solutions for risk management but within strict compliance boundaries.
Audience	Security professionals, compliance teams, and organizations requiring regulated standards.	Financial institutions, ICT service providers, and critical financial infrastructure operators in the EU.
Example Guidelines	NIST SP 800-190 (Application Container Security Guide), SP 800-218 (SSDF).	Incident reporting protocols, ICT risk management requirements, operational resilience testing.
Incident Focus	Resilience under attacks and secure incident management.	Ensuring financial stability and ICT continuity during operational disruptions.
Collaboration with DevOps	Encourages collaboration via DevSecOps to integrate security into DevOps processes.	Requires formal governance structures for ICT risk and resilience, with less emphasis on DevOps-specific practices.