HORIZON3

Demonstrating DORA Resilience in the Financial Sector

How Financial Services Firms Can Support Regulatory Requirements With Evidence-Based Security

WHITEPAPER

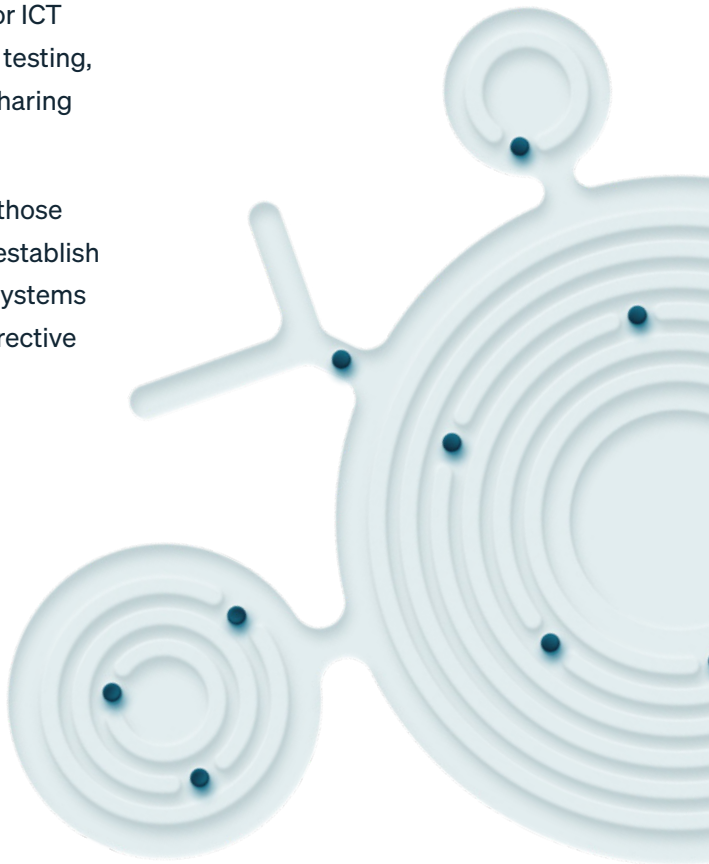
DORA Is Now an Operational Requirement

The EU's Digital Operational Resilience Act (DORA) has applied since January 17, 2025, raising the bar for how financial institutions manage, monitor, and demonstrate their digital operational resilience. Financial entities within its scope must address their ability to withstand, respond to, and recover from disruptions involving information and communication technology.

Information and communication technology (ICT) encompasses the systems, software, networks, and services used to manage, process, and transmit data. For financial institutions, these resources support transactions, customer access, and daily operations. Managing their security and resilience requires attention to both internal systems and dependencies on third-party providers.

DORA covers a broad range of financial entities, including banks, investment firms, insurers, and authorized crypto-asset service providers, subject to its scope and exemptions. It establishes requirements for ICT risk management, incident reporting, digital operational resilience testing, and ICT third-party risk management, alongside a framework for sharing cyber threat information.

For security leaders and practitioners, the challenge is translating those obligations into operational practice. Policies and documentation establish responsibilities and processes. Testing provides evidence of how systems and controls perform, where weaknesses remain, and whether corrective actions worked.



What DORA Requires

DORA is commonly organized around five core pillars:

1 ICT Risk Management

Establish and maintain a framework to identify, protect against, detect, respond to, and recover from technology-related risks.

2 ICT Risk Management

Maintain processes to detect, manage, and classify ICT-related incidents and report major incidents to the relevant authorities.

3 Digital Operational Resilience Testing

Conduct risk-based testing of systems, controls, and processes. Selected financial entities must also undertake advanced threat-led penetration testing under specific regulatory requirements.

4 ICT Third-Party Risk Management

Assess and manage risks arising from technology providers, including contractual obligations, concentration risk, and exit arrangements.

5 Information Sharing

Enable voluntary sharing of cyber threat information and intelligence within trusted communities, subject to safeguards for confidentiality, personal data, and competition.

The Risk of Assumed Resilience

DORA requires financial entities to manage ICT risk and test their digital operational resilience. Policies, audit records, and tabletop exercises contribute to that work, but they do not alone establish whether attackers can exploit weaknesses in live systems. Gaps can include:

- → Assumed effectiveness of security controls that have not been tested against attacker behavior.
- → Overreliance on documentation without technical evidence of how controls perform.
- → Blind spots across hybrid environments, identity systems, and lateral movement paths.
- → Insufficient testing of vendor-managed systems, third-party access, and cloud configurations.

Attackers can combine weak credentials, misconfigurations, and excessive privileges to reach critical systems and sensitive data. A control may be deployed and documented yet fail to prevent that progression. Testing helps reveal the difference between a control's intended protection and its demonstrated effectiveness.

For financial institutions, obtaining that evidence must also account for operational continuity. Testing needs clear scope, appropriate safeguards, and methods suited to production environments. The objective is to expose weaknesses without putting the services customers depend on at unnecessary risk.

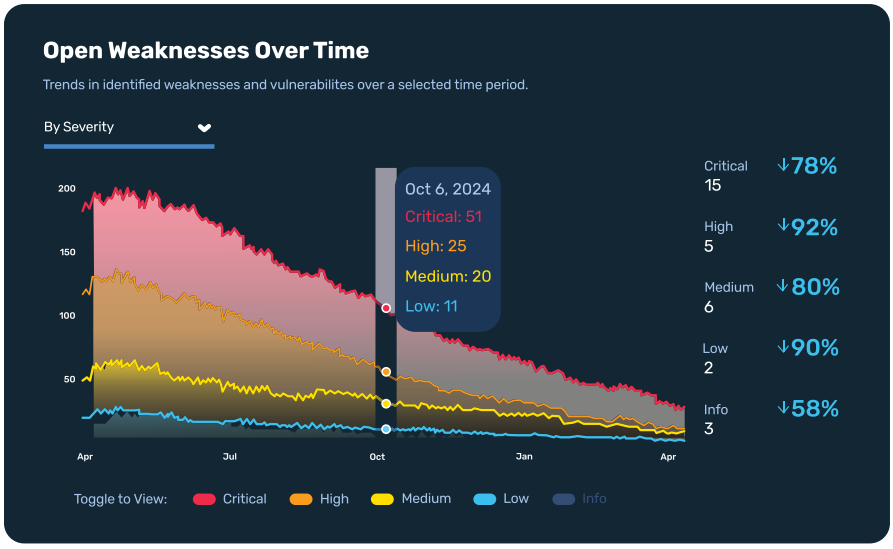
Repeatable security testing helps teams identify these gaps as environments change and verify that corrective actions worked. It contributes evidence to a broader resilience program that also addresses incident management, continuity, and recovery. Without that evidence, organizations may overestimate their protection and leave exploitable paths to disruption unresolved.

How NodeZero Helps Firms Meet DORA Head-On

NodeZero, the Proactive Security Platform from Horizon3, helps financial institutions support DORA-related testing and risk management through autonomous, production-safe security validation.

Production safety has been NodeZero's highest engineering priority since the beginning. Engineered guardrails and prevalidated actions support repeatable testing against live systems, backed by a track record of use in real production environments.

NodeZero uses attacker techniques to uncover exploitable weaknesses, including weak credentials, exposed assets, misconfigurations, and privilege escalation paths. It connects those findings to demonstrated impact so teams can prioritize corrective action.



NodeZero Enables Firms To:



Test ICT security controls
Determine whether attackers can overcome controls, rather than relying solely on evidence that they are deployed.



Assess segmentation and access controls
Test whether attackers can cross network boundaries or expand access across on-premises and cloud systems.



Demonstrate attack paths
Chain weaknesses from initial access through lateral movement to show which systems and data an attacker could reach.



Verify remediation
Retest identified weaknesses after changes to confirm whether fixes closed the exposure.



Support third-party risk assessments
Test authorized vendor-managed systems and third-party access paths within an agreed scope.



Document findings and progress
Generate reports and dashboards that support remediation tracking, executive oversight, and compliance evidence.

These capabilities contribute to a broader DORA resilience program. They complement formal threat-led penetration testing where required, alongside the organization's incident reporting, continuity, recovery, and third-party governance processes.

NodeZero Across the Org Chart

DORA places responsibility for ICT risk management on the management body, while implementation depends on coordinated work across security, technology, compliance, and risk teams. NodeZero helps connect technical execution with executive oversight through evidence each group can use.

For engineers and security practitioners, offensive testing provides concrete findings: exploitable weaknesses, lateral movement paths, and demonstrated access to systems and data. Teams can investigate how an attack succeeded, identify where to intervene, and verify whether their changes worked.

For executives, compliance leads, and risk stakeholders, those results support decisions about priorities, resources, and accountability. Evidence of exposure and remediation progress helps leaders understand where action is needed and communicate the results of security investments.

NodeZero brings these perspectives together. It uses attacker techniques to validate exposure in production environments, then translates the findings into remediation guidance, reports, and dashboards. NodeZero Insights aggregates results across tests, helping leaders track trends and identify recurring issues that may require broader policy or control changes.

This shared evidence connects the weaknesses practitioners address with the risks leaders need to oversee.

Aligning NodeZero With DORA Activities

NodeZero supports specific testing, risk management, and evidence-gathering activities within a broader DORA program.

DORA-Related Activity	How NodeZero Helps
ICT Risk Management	Identifies exploitable weaknesses and demonstrates paths to critical systems and sensitive data, helping teams prioritize corrective action.
Detection and Response Validation	Generates controlled attacker activity that teams can use to assess whether security tools and operational processes detect and respond as intended.
Digital Operational Resilience Testing	Provides repeatable, production-safe penetration testing to uncover attack paths and reassess exposure as environments change.

ICT Third-Party Risk Management	Tests authorized vendor-managed systems and third-party access paths to provide technical evidence that supports due diligence and ongoing oversight.
Remediation and Verification	Provides actionable guidance and targeted retesting to establish whether fixes addressed the identified weaknesses.
Governance and Reporting	Consolidates findings and remediation progress into reports and dashboards that support management oversight and audit preparation.

These contributions support DORA implementation without replacing its broader obligations. Autonomous penetration testing alone does not satisfy formal threat-led penetration testing requirements or establish the effectiveness of incident reporting, business continuity, and recovery arrangements.

Advanced NodeZero Capabilities That Support Resilience

Beyond core penetration testing, NodeZero provides capabilities that help financial institutions focus assessments on critical assets, understand sensitive data exposure, and track remediation progress.

- **High-Value Targeting:** Identifies high-value accounts and systems and tests whether attackers can reach or compromise them, helping teams focus on assets that support critical financial services.
- **Advanced Data Pilfering:** Finds and validates sensitive data exposure, demonstrating which customer records, credentials, and financial information attackers could access.
- **NodeZero WebApp:** Tests custom web applications, including authenticated workflows, for exploitable business logic, access control, and session weaknesses. Provides evidence developers can use to investigate and remediate findings.
- **Active Directory Password Audit:** Identifies weak passwords, helping teams address credential exposure that could enable unauthorized access and lateral movement.
- **Endpoint Security Effectiveness:** Tests whether endpoint security tools detect and stop attacker behaviors in production environments, helping teams identify gaps and improve control configurations.
- **NodeZero Insights:** Consolidates pentest results into dashboards that track exposure, remediation progress, and recurring weaknesses, supporting executive oversight and decisions about security priorities.

Together, these capabilities help teams connect technical findings to the systems, data, and services that matter most, while providing evidence to support ongoing risk management and resilience testing.

Conclusion: Demonstrate Resilience With Evidence

DORA makes digital operational resilience an ongoing responsibility. Financial institutions need to understand their exposure, address weaknesses, and demonstrate progress while maintaining the services customers depend on. Policies and assessments support that work, but their value grows when backed by evidence of how security controls perform.

NodeZero helps financial organizations build that evidence through autonomous testing grounded in production safety. It demonstrates exploitable attack paths, guides remediation, and verifies whether fixes worked. Practitioners gain clear priorities for corrective action, while leaders gain visibility into exposure and measurable security progress.

Incorporating this testing into a broader DORA program helps connect governance with operational practice. Financial organizations can reassess exposure as environments change, document improvements, and make informed decisions about protecting critical systems and customer data.

DORA resilience requires evidence. Start with what attackers can exploit.

Schedule a demo to see how NodeZero can support your security testing and DORA compliance efforts.

https://horizon3.ai/schedule-demo