elastio

Countdown to Comply with DORA

How Elastio Can Help Your Business Be Compliant by January 2025

The Digital Operational Resilience Act (DORA) is the EU's answer to rising cyberattacks on financial institutions. Recognizing the inevitability of cyber disruption, DORA mandates resilience requirements for European financial entities to ensure that their services can withstand cyberattacks.

There is great pressure on institutions to demonstrate that their business is adequately compliant with these regulations, before they go into effect in January 2025. Fortunately, Elastio can help.

DORA: A Quick Guide

DORA encompasses four main pillars: ICT Risk Management, ICT-Related Incident Reporting, Digital Operational Resilience Testing, and Managing ICT Third-Party Risk. Elastio's proactive inspection of backup data for ransomware addresses key requirements across these pillars. Here's how:

How Elastio Can Help

1. ICT RISK MANAGEMENT:

Financial entities must establish resilient ICT systems and protocols to proactively manage and mitigate risks

Continuous Threat Detection (Article 10): Elastio's proactive inspection of backups for ransomware provides an additional layer of threat detection beyond perimeter defenses, such as EDR/XDR, which are often bypassed by increasingly sophisticated hackers. Our adaptive RansomwareIQ AI/ML engine, built by reverse-engineering every known form of ransomware, is uniquely equipped to identify ransomware - even novel threats - with 99.99% accuracy. Elastio's ability to create alerts for proactive actioning also addresses SIEM and SOAR requirements.

Assure Business Continuity (Article 11): Elastio helps companies quickly resume business activity in the event of an attack by automatically directing you to your last-known clean copy of data (2 A-C.). Elastio's reporting on incident scope and on the age of last-known clean, thereby the extent of data loss, also enables companies to perform preliminary impact analysis (2 D).

Safe Backup Restoration & Recovery (Article 12): DORA mandates that backup data is stored in systems that are logically segregated from the source system and that the activation of backup systems does not jeopardize the security of the business. By validating the integrity of data before it is backed up and stored in a secure, immutable vault, Elastio assures that businesses always know their backups are clean and safely recoverable in the event of attack, protecting against the risk of reinfection.

2. ICT-RELATED INCIDENT REPORTING

Under DORA, financial entities must swiftly report ICT-related incidents to both internal management and relevant EU authorities.

Cyber Threats Classification (Article 18): DORA mandates that financial entities classify cyber threats based on factors like impact and data loss. Elastio enhances this process by offering precise insights into compromised files and the last clean recovery point, ensuring a thorough understanding of the incident's scope and its associated data loss.

Detailed Alerts on Nature and Scope of Attack (Article 19): Elastio provides compliance teams with critical details about affected files and specific ransomware variants, enabling comprehensive incident reporting. Reports are customized based on the incident's severity, ensuring the appropriate level of detail is provided to regulators, partners, and clients, tailored to their specific needs.

3. ICT-RELATED INCIDENT REPORTING

Under DORA, financial entities must swiftly report ICT-related incidents to both internal management and relevant EU authorities.

Recovery Testing (Article 25): DORA mandates that companies test their business continuity at least yearly. Regular recovery testing is a cornerstone of Elastio's offering. By continuously validating recovery plans, organizations can ensure their systems are resilient and can be restored effectively after a disruption. Elastio also integrates seamlessly with AWS Restore Testing to provide automated recovery testing.

Continuous Improvement: Through frequent testing and validation, organizations can identify weaknesses in their recovery plans and make necessary improvements. This continuous cycle of testing and enhancement strengthens overall resilience over time.

4. MANAGING OF ICT THIRD-PARTY RISK

DORA stresses the importance of managing third-party ICT service providers by ensuring they comply with DORA's resilience requirements.

Vendor Assurance: When third-party ICT service providers utilize Elastio's services, it provides assurance that backups managed by these vendors are secure and free from ransomware. This reduces third-party risks and ensures that all parties involved in the data lifecycle adhere to high standards of operational resilience.

Moreover, DORA holds executive leadership accountable for compliance, making proactive oversight essential. Elastio strengthens businesses' security governance and oversight with:

Comprehensive Reporting: Generate detailed reports on backup integrity, age of last-known clean (and therefore potential data loss in the event of an attack) and recovery tests, demonstrating DORA compliance and providing clear evidence to oversight bodies.

Board-Level Insights: Equip executives with actionable insights to guide discussions and decisions on ICT risk management, ensuring they are fully engaged in resilience efforts.

Secure your compliance and elevate your resilience today.

With the January 2025 DORA compliance deadline approaching, financial institutions need to act now. Elastio is your partner in navigating the EU's new digital resilience standards.

Our cutting-edge threat detection, backup integrity verification, detailed incident reporting, and continuous testing keep your business ahead of cyber threats and operational risks.

In an era where digital threats are growing more sophisticated by the day, adhering to regulations like DORA goes beyond mere compliance—it's about securing the very future of financial institutions.

Partner with Elastio to meet DORA requirements with confidence and safeguard your operations against future cyber challenges. Don't just comply—thrive.