

Ensuring Operational Resilience and Data Protection with the VAST Data Platform:

A Guide to DORA Compliance for CIOs



The Digital Operational Resilience Act (DORA) is a regulation established by the European Union as part of its Digital Finance Package, designed to enhance and enforce the operational resilience of financial entities across the EU. DORA became law in January 2023 under Regulation (EU) 2022/2554, with compliance required by January 2025.

DORA is a well-intentioned regulation aimed at protecting the interests of the EU and its global partners. At its core is the principle of being “commensurate to the risk,” a point mentioned multiple times throughout the regulation.

DORA has Fangs

DORA enforces strict compliance measures, holding CIOs directly accountable for ensuring Information and Communication Technology (ICT) resilience and data protection. Non-compliance can lead to severe penalties, including fines and operational restrictions. The requirement for public disclosure of non-compliance applies additional pressure to governing executive management teams.

Commensurate to the ICT Risk

DORA specifies that the most critical ICT risks must receive the highest level of attention.

Per the European Union Agency for Cybersecurity (ENISA) report “*ENISA THREAT LANDSCAPE 2024*,” the top threats include:



Ransomware



Malware



Social Engineering

While businesses have the right to reassess their own risk profiles, it would be prudent to align with the recommendations of the ENISA, as Lead Overseers—supervisory authorities appointed by the EU—will likely rely on this guidance in their assessments.

Preparation and Compliance

DORA focuses heavily on testing and review of the covered entities by a Lead Overseer, who is charged with ensuring an entity's compliance with DORA. Key areas of focus include:

1) Ransomware Recovery

The VAST Data Platform delivers the resilience required to meet audit standards and ensure rapid recovery from ransomware attacks. With an industry-leading recovery rate of over 360TB per hour for a typical entry level cluster configuration, VAST Data offers unparalleled speed and efficiency, making it a critical asset for demonstrating DORA compliance. Without this level of performance, other platforms may struggle to recover production applications swiftly enough to meet regulatory demands.

Example

ERP System	Enterprise Resource Planning	250 TB
Platform	Speed	~ Time to Recover
Legacy	~8 TB/hr	1875 Minutes (31.6H)
VAST Data*	360 TB/hr	41 Minutes

**even faster possible with more nodes*

Additionally, the VAST Data Platform supports immutable snapshots across all protocols, providing robust protection against data tampering and ensuring the integrity of your backups. Combined with Compliance WORM lock integration from leading data protection ISVs, VAST provides a multi-layered approach to data protection.

2) Ransomware and Malware Detection

The Lead Overseer will look for advanced anomaly detection systems that leverage AI/ML capabilities to proactively identify and respond to ransomware and malware threats in real-time.

The VAST Data Platform integrates deep learning models for monitoring data patterns, enabling rapid detection of anomalies associated with ransomware and malware activities. This capability ensures compliance with DORA's requirements for proactive threat management and immediate incident response.

3) Social Engineering

The Lead Overseer will evaluate the organization's preparedness against social engineering attacks, such as phishing, which often serve as entry points for cyber threats.

The VAST Data Platform supports comprehensive audit trails and multi-layered access control (including Attribute-Based Access Control or ABAC), ensuring any suspicious or unauthorized access attempts are flagged and investigated immediately. By reinforcing user validation and monitoring access behaviors, VAST Data ensures entities can mitigate social engineering risks and demonstrate compliance with DORA's security expectations.

The VAST Way

Exceed the Lead Overseer's Expectations with VAST Data's Unmatched Resilience and Recovery.

By choosing the VAST Data Platform, your organization doesn't just meet the stringent requirements of DORA—you exceed them. VAST Data offers unparalleled resilience and rapid recovery capabilities that not only satisfy Lead Overseers but set a new standard in operational excellence. With advanced threat detection, lightning-fast data recovery, and robust protection against cyber threats, VAST Data empowers CIOs to confidently navigate the complexities of digital operational resilience. Trust in VAST Data to fortify your enterprise, ensuring compliance today and securing your organization's future in an ever-evolving digital landscape.

[Learn about VAST Data Protection and our customers.](#)

[Discover VAST Data's quick data center deployment story with Colossus at xAI.](#)



[Scan Here](#) learn more.