VERITAS

DORA

Risk Management

White Paper | August 2024

Contents

Executive Summary

Implementing a robust risk management strategy is crucial for ensuring the security and stability of financial institutions. A cyberattack on the financial sector could result in devastating consequences, so the European Union (EU) is working to strengthen cyber resiliency through the Digital Operational Resilience Act (DORA).

By adhering to DORA regulations, organizations can enhance their cybersecurity measures, mitigate risks, and strengthen their overall operational resilience. This proactive approach not only safeguards the financial institution but also helps maintain trust with clients and stakeholders. In today's digital age, where cyber threats are constantly evolving, DORA plays a vital role in fostering a secure and resilient environment within the financial sector.

Starting January 17, 2025, this new EU legislation will apply to a broad range of financial entities, including banks, payment institutions, investment firms, crypto services, and third parties that provide information and communication technology (ICT) systems and services. DORA is intended to help organizations in the financial sector improve their resilience, focused on securing ICT. To comply with DORA, financial firms and third parties must prove they are:

- Cyber-resilient and their security posture can deliver the required digital operation resilience, and
- They have a governance framework in place to manage risk.

Compliance with global regulations is complex, with high penalties for non-compliance. Enterprises with high levels of non-compliance showed an average cost of USD$5.05 million, exceeding the average costs of a data breach by 12.6%, according to 2023 IBM Cost of Data Break Report. At Veritas, we specialize in helping enterprises achieve compliance with leading data security, protection, and governance solutions for cyber resilience.

This whitepaper provides a comprehensive overview of what enterprises need to consider in their journey toward DORA compliance, emphasizing the integration of Veritas solutions. Key areas covered include understanding DORA's applicability, mapping specific processes and controls to meet DORA requirements, and securing data across all infrastructure types—on-premises, cloud, and hybrid environments.

DORA Facts

- DORA became effective on January 16, 2023, and will be enforced starting from January 17, 2025.
- DORA is intended to strengthen the IT security of financial entities across the EU. The legislation defines financial entities into 20 types of entities and ICT third-party service providers, including banks, insurance companies, investment firms, payment services providers, Crypto-Asset Service Providers, Credit Institutions, Credit rating agencies, Crowdfunding Service Providers, and Critical Third-Party Providers.
- There are 5 pillars of DORA, 64 total articles, and 106 recitals.
- Regulation applies to all member states of the European Union and to all corporations that operate in those countries.
- DORA is supervised by the three European Supervisory Authorities (ESAs):
  - European Banking Authority (EBA)
  - European Securities and Markets Authority (ESMA)
  - European Insurance and Occupational Pensions Authority (EIOPA)

The Five Pillars of DORA

Let us take a step back and understand what DORA is and, most importantly, what is expected from the EU financial industry. The DORA regulation aims to ensure full alignment between financial entities' business strategies and how they manage ICT risk. Managing bodies are pivotal in steering ICT risk and the digital resilience strategy.

The regulation is intended to strengthen the IT security of financial entities such as banks, insurance companies and investment firms and make sure that the financial sector in the EU can stay resilient in the event of a severe operational disruption. DORA synchronizes operational resilience rules for the financial sector, covering 20 types of financial entities and third-party ICT service providers.

- **ICT Risk Management and Governance**

This foundational pillar mandates a thorough identification, assessment, and mitigation of ICT risks, necessitating entities to establish robust internal governance and control frameworks.

- DORA clearly establishes that an entity's management body is responsible for ICT management. This includes board members, executives, and senior managers. They must establish and implement risk management strategies. Failure to comply could lead to personal accountability.
- Continuous risk assessment frameworks will be required. The ability to identify and classify all critical data is mandatory with clear documentation of dependencies required.
- Business impact analysis is required, especially in the case of cyberattacks and disasters. Business continuity and disaster recovery plans are mandated, with rules regarding data backup and recovery, the restoration process, and communications plans.
- Cybersecurity protection measures are required, including policies around IAM (Identity and Access Management), anomaly detection, malware scanning, threat response, data insights, SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), and patch management.

- **ICT-Related Incident Management**

This pillar emphasizes the quick and effective handling of operational disruptions or cyber incidents. It requires organizations to set up a smooth process for detecting, managing, and promptly reporting major cyber incidents.

- Reporting of major incidents is mandatory. Entities are required to file three different kinds of reports for critical incidents: an initial report notifying authorities, a second report on progress toward resolution, and a third and final report that analyzes the root causes of the incident.

- **Digital Operational Resilience Testing**

This pillar requires regular tests of organizational resilience to ensure preparedness against a wide spectrum of ICT risks. It mandates comprehensive testing programs to identify, address, and mitigate vulnerabilities.

- Entities must perform vulnerability and scenario-based testing yearly. Threat-led penetration testing (TLPT) is an additional requirement every three years for those deemed critical to the financial system.

- **Third-Party Risk Management**

In today's interconnected financial ecosystem, third-party service providers play a critical role. Financial firms are now expected to take an active role in managing ICT third-party risk and developing specific contractual arrangements for important and critical functions.

- DORA requires entities to conduct thorough third-party service provider assessments, map their dependencies, ensure security and integrity, and make arrangements for clear exit strategies. Meaningful plans must be in place for transitioning data, applications, and services from a cloud computing environment back to on-premises or to another cloud provider.
- Contracts are not allowed with entities that do not meet these requirements.
- Entities will be empowered to forbid providers from entering into contracts with those that don't comply with DORA.

- **Information Sharing**

This pillar champions the exchange of cyber threat intelligence among organizations to foster a collective resilience against cyber threats. By encouraging a culture of collaborative information sharing, it aims to elevate the sector's overall preparedness and response capabilities.

DORA Non-Compliance

Non-compliance with the DORA pillars is not advisable. DORA enforces strict penalties to ensure digital operational resilience for financial institutions. Failure to comply with DORA regulations can have severe penalties, reflecting the Regulation's strict position on cyber resilience.

- Financial penalties: the cost of non-compliance
  DORA establishes rigorous financial penalties for violations of its requirements. A breach could see institutions fined up to **2%** of their total annual worldwide turnover or up to 1% of the company's average daily turnover worldwide. Individuals and companies could face fines of up to **€1.000.000**. Critical third-party ICT service providers, integral to financial entities, could incur even higher fines—up to **€5.000.000** or **€500.000** for individuals if they fail to meet DORA's stringent standards.
- Potential for criminal sanctions
  Member States can impose criminal penalties for breaches of DORA, as per Article 52. States must ensure measures are in place to enable liaising with judicial, prosecuting, or criminal justice authorities to implement these penalties effectively. DORA's penalty structure fortifies the financial sector against cyber threats. By integrating penalties with preventive measures and reporting obligations, experts behind DORA ensure a resilient economic ecosystem and maintain its participants' integrity and trust. Without a doubt, this makes DORA readiness even more critical.
- Authority to impose penalties
  European Supervisory Authorities (ESAs) are responsible for imposing penalties. They are empowered by DORA to uphold digital operational resilience in the financial industry. As stipulated in Article 97, competent authorities have the necessary supervisory and investigatory powers and the ability to publish notices of administrative penalties, ensuring transparency and accountability.
- Designated entities and timeframe
  These penalties and the framework that dictates them were published in the Official Journal of the European Union on December 27, 2022, under Regulation (EU) 2022/2554. The regulatory requirements become enforceable on **January 17, 2025**, allowing institutions to align their operations with DORA's mandates. ESAs will develop and adopt technical standards that specify compliance requirements during this period.
- Operational readiness and business presence
  Critical ICT third-party service providers established outside the EU must ensure an adequate business presence within the EU to facilitate oversight and ensure that penalties can be effectively imposed and enforced. This provision, detailed in paragraph 81, requires designated critical service providers to establish a subsidiary in the EU within **12 months** of their designation.
- Hybrid funding for oversight tasks
  The ESAs may incur costs before the start of the Oversight Framework, for which a hybrid funding model is proposed in paragraph 96. Contributions from the Union and national competent authorities will fund the development of dedicated ICT systems supporting oversight.

Why Veritas?

Veritas is at the forefront of delivering simplified, resilient solutions that protect IT systems and ensure data integrity throughout their lifecycle. With expertise in navigating complex regulatory landscapes and robust data protection requirements, we offer advanced capabilities such as AI-based classification and anomaly detection. These technologies provide deep insights into data usage and behavior, which is essential for compliance with regulations like the Digital Operational Resilience Act (DORA). Our solutions not only mitigate risks and eliminate vulnerabilities but also enable seamless scalability, upgrades, and maintenance. From edge to core to cloud, Veritas supports a secure digital environment and integrates backup and recovery as a pivotal component of a robust, multi-layered cybersecurity strategy.

Veritas Capabilities for DORA Compliance: Enhancing Resilience and Compliance

Veritas offers advanced capabilities tailored to strengthen cybersecurity resilience and ensure compliance with the DORA.

Pillar 1: ICT Risk Management

The Veritas data management solution offers in-depth insight into your financial organization's data. It conducts two levels of file scans. First, it analyzes metadata to understand file age, type, usage, and ownership. Then, it performs deep scans to read and classify the content using Optical Character Recognition (OCR) and AI based on a wide range of pre-built and custom policies. This enables administrators to prioritize data recovery based on content relevance and comprehend potential data risks.

Pillar 2: Incident Reporting

Unlike traditional anomaly detection, our solution uses entropy-based anomaly detection on both data and user behavior. Additionally, it automatically adjusts adjusts multi-factor authentication (MFA) and multi-party authentication (MPA) security settings to defend against potential insider attacks. Our capabilities integrate vulnerability assessments and scenario-based testing for incident management and resilience. This comprehensive approach provides administrators with insights and an early warning system to address security challenges, ensuring ongoing operational resilience, which is essential for meeting incident reporting and resilience testing mandates.

In addition to incident reporting, our eDiscovery capabilities are designed to conduct thorough investigations and automate up to 100 simultaneous searches. It can process and analyze over 500 file types with streamlined workflows, ensuring secure scalability through content isolation and export. With built-in immutability and advanced redaction features, organizations can swiftly respond to regulatory requests, empowering compliance officers and legal IT staff to make informed decisions and mitigate risks effectively.

Pillar 3: Digital Operational Resilience Testing

To support strong risk management practices, our solution enables regular reviews and audits to ensure that the measures in place are effective and comply with regulatory requirements for incident reporting and resilience testing. Veritas solutions improve Digital Operational Resilience Testing through real-time anomaly detection, continuous threat response capabilities, and strong resilience against cyber incidents, all strictly adhering to DORA guidelines.

Implementing a comprehensive testing framework, which includes vulnerability assessments, penetration testing, and scenario-based testing, is essential to achieving high availability and scalability in data protection and application resilience. Our solution's resiliency rehearsals feature allows this testing without disrupting the production environment.

Our solution streamlines the process of thoroughly analyzing test results to identify weaknesses and areas for improvement, ensuring that any findings related to recovery point objectives (RPO) and recovery time objectives (RTO) are promptly reported to senior management and stakeholders for remediation. This approach facilitates proactive management of resilience testing outcomes, enhancing overall operational readiness.

Pillar 4: Third-Party Risk Management

Veritas capabilities enable financial firms to manage ICT third-party risks actively, ensuring compliance with DORA's requirements for third-party service provider assessments, security, and robust contractual arrangements safeguarding data integrity. Secure archiving and information governance practices facilitate comprehensive data archiving from diverse sources and platforms, which is crucial for maintaining data integrity and readiness for compliance audits. These solutions support ICT risk management alignment with DORA, conducting regular audits and assessments of third-party service providers to meet stringent security and regulatory standards, including those mandated by GDPR. Leveraging a Zero-Trust architecture and immutable storage enhances resilience against external threats, automating data protection and ensuring swift verification of recovery operations in line with DORA's security mandates for managing third-party risks.

Pillar 5: Information Sharing

Veritas enhances Information Sharing capabilities through advanced tools that provide deep insights into data usage and behavior. These capabilities support proactive ICT Risk Management and Incident Reporting by enabling organizations to prioritize critical data for protection and recovery based on its relevance and sensitivity. Additionally, our platform for eDiscovery streamlines data capture and retention across multiple communication channels, ensuring compliance with regulatory requirements like DORA and GDPR. Advanced threat intelligence feeds enable swift detection and response to emerging threats, aligning with DORA's emphasis on continuous monitoring and threat response. These integrated solutions empower financial institutions to securely share information, mitigate risks effectively, and maintain regulatory compliance.

A Call to Action

The integration of cyber recovery solutions is not a luxury; it's a strategic necessity in today's threat landscape. The mission extends beyond protecting your organization's digital assets. We must also ensure that our defense mechanisms are DORA-compliant. The solution must be intelligent, agile, and integrated, as the EU financial industry faces many threats. Cybersecurity spending is predicted to exceed $1.75 trillion cumulatively from 2021 to 2025. This underscores the scale of investment in combating these threats and the importance of strategic integration within cybersecurity efforts.

Now is the time to work with your broader organization to ensure you are managing your risk. Our solutions are not just about recovery; they're about empowering your SecOps (Security and Operations) team with the tools and integrations necessary to defend against today's threats and anticipate tomorrow's challenges.

Explore Veritas 360 Defense to discover how Veritas can help you control your data, increase resilience against cyberthreats, and ensure compliance. Learn more about using our comprehensive solutions to build a more secure future for your data.

Remove doubt that you will be resilient from a cyberattack by completing the cyber recovery checklist. It provides a phased approach so that you know where to start and how to prioritize.

A way you can stay current on a wide range of cybersecurity topics is to subscribe to the Veritas Cybersecurity Newsletter on LinkedIn for insights on enterprise-grade cyber resilience.

About Veritas

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on X at @veritastechllc.

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact