DORA

Get Prepared

Executive Summary

The Digital Operational Resilience Act (DORA) was introduced in January 2023 and goes into full effect on January 17, 2025. It was created to provide legal guiderails for financial entities and their preferred Information Communication Technologies (ICT) providers as it relates to cybersecurity and resilience. This regulation aims to provide stability and foresight within the financial industry to reduce the risk of cross industry and economic impact of a cyber-attack.

The structure of DORA is designed to ensure the resilience of financial entities in the face of today's cyber threat landscape. It is organized by five pillars of compliance including:

1. ICT Risk Management
2. ICT-Related Incident Reporting
3. Digital Operational Resilience Testing
4. Management of ICT Third-Party Risk
5. Information and Intelligence Sharing

These all come together to ensure the ability to recover critical and important information and functions in a timely manner. Additionally, it requires the ability to test and prove that recovery processes will be successful and in compliance. Will your current data protection architecture allow you to meet your current recovery requirements, and be compliant? Veritas is here to help you get prepared.

How Can Organizations Prepare for DORA Compliance?

While DORA requirements will continue to evolve between now and January of 2025, don't delay preparing for this new regulation. Now is the time to ensure that your organization is ready to take the actions necessary to achieve compliance. Planning for and executing a compliance plan for DORA offers many benefits for your organization, including:

- Better mitigation of cybersecurity threats and related risks.
- Being able to recover from ICT-related disruptions faster and more effectively.
- Avoiding non-compliance fines and penalties altogether.

Complying with DORA spans multiple risk management functions:

Cyber risk and controls compliance management

DORA focuses on ICT and ICT third-party risk. It is a cybersecurity and information technology regulation at its core. This means organizations should take stock of their cyber risk landscape now and begin working to bolster their cybersecurity defenses to prevent and respond to ICT incidents.

From a compliance point of view, organizations need to implement a proven cybersecurity framework, and enable the processes and technology needed to streamline DORA compliance.

Third-party risk management

Reducing ICT risk and hardening a financial institutions ICT security against a systemic shock is the goal of DORA. Financial institutions leverage several third-party ICT service providers. Because of this, DORA aims to institute improved cyber security processes for vetting and onboarding third parties and vendors. It is expected that DORA will impose requirements surrounding the contracting and ongoing monitoring of third parties. Proactively automating these processes using modern risk management technologies will save on time and ensure accuracy of reporting when DORA requests proof of compliance.

Incident management

DORA will increase the burden on organizations to report ICT-related incidents in a timely fashion, and such incidents are increasing exponentially. Organizations will likely find themselves producing more reports more frequently than ever before. To eliminate draining your cybersecurity and compliance teams, it is crucial to build an automated process to generate these reports.

Operational resiliency and business continuity planning

DORA regulators have made it clear that they expect organizations to have strong business continuity plans in place. A strong plan includes a regular cadence for testing operational resilience. The time to start developing these plans is now. Start looking for ways to automate your testing where possible.

DORA also requires organizations to have processes for becoming educated on ICT third-party risk, as well as analyzing and learning from ICT-related incidents. Cyber risk quantification is a powerful tool for tying ICT third-party risk to potential financial impact and helping communicate in a common, relatable language. Discuss the potential impact ICT third-party risk could have on your organization now. This will ensure that the compliance team understands the importance of supporting and complying with the DORA regulations.

DORA's Impact:

- **Increased costs for the financial institutions:** Investments in technology, personnel, and compliance efforts will be necessary.
- **Improved overall security posture of the EU financial sector:** More robust ICT risk management practices will lead to increased resilience.
- **Potential for innovation:** New technologies and solutions may emerge to address the challenges posed by DORA.

Make An Action Plan for DORA Compliance

DORA, the Digital Operational Resilience Act, brings significant changes to how EU financial institutions manage their information and communication technology (ICT) risks. It is crucial to develop a comprehensive action plan to ensure compliance and enhance your organization's overall resilience. Here's a framework to guide your planning:

1. Assess Your Current State:

- *Gap Analysis:* Identify areas where your existing practices fall short of DORA requirements. This includes ICT risk management, incident reporting, penetration testing, outsourcing, and information sharing protocols. This should be an internal process, however, aided by technology. Veritas provides tools such as IT Analytics that can map your infrastructure and provide reports for gap analysis and proving compliance further in the process.
- *Inventory & Mapping:* Compile a detailed inventory of ICT assets, systems, and dependencies. Map them to relevant DORA provisions to understand specific compliance needs. Be aware that specific requirements based on further classification on the type of financial entity may arise. An ideal tool set for this process would be Veritas Data Insight. It allows organizations to inventory their data by scanning and classifying the data in the wild. Understanding the organizations data, allows the security team to prioritize the data for recovery.

2. Build a Compliant Framework:

- *ICT Risk Management:* Develop a robust ICT risk management framework aligned with DORA's principles. This includes risk identification, assessment, mitigation, and monitoring procedures.
- *Incident Reporting:* Establish clear procedures for timely reporting of major ICT incidents to regulators, adhering to DORA's reporting thresholds and timelines.
- *Penetration Testing & Vulnerability Assessments:* Implement regular penetration testing and vulnerability assessments on critical systems and infrastructure to identify and address vulnerabilities proactively.
- *Information Sharing & Cooperation:* Foster a culture of information sharing within your organization and with relevant stakeholders, including peer institutions and regulators, as permitted by DORA.
- *Outsourcing Management:* Establish stringent criteria and oversight mechanisms for outsourcing ICT functions to third-party vendors, ensuring compliance with DORA's outsourcing requirements.

3. Prioritize & Implement:

- *Risk-Based Approach:* Prioritize your initiatives based on the severity and likelihood of identified risks. Focus on addressing critical vulnerabilities and compliance gaps first.
- *Phased Implementation:* Develop a phased implementation plan with achievable milestones and deadlines. Consider resource constraints and potential disruption to ongoing operations.
- *Project Management:* Assign clear ownership and accountability for each initiative. Utilize project management tools and techniques to track progress and ensure timely completion.

4. Training & Communication:

- *Employee Awareness:* Train employees on DORA's requirements and their role in upholding the organization's cybersecurity posture. Foster a culture of security awareness and incident reporting.
- *Leadership Engagement:* Secure buy-in and support from senior management. Communicate the importance of DORA compliance and its benefits for the organization's overall resilience and reputation.
- *Regulatory Liaison:* Maintain close communication with relevant regulators to stay informed about DORA interpretations and updates.

5. Continuous Improvement:

- *Regular Reviews & Audits:* Conduct periodic reviews of your DORA compliance framework and practices. Utilize internal and external audits to identify areas for improvement.
- *Testing & Drills:* Regularly test your incident response plans and communication protocols to ensure effectiveness and preparedness for real-world scenarios.
- *Embrace Innovation:* Continuously seek new technologies and solutions that can enhance your ICT risk management capabilities and compliance posture.

DORA compliance means integrating cyber recovery considering both the needs of the organization as a whole and the compliance team. This seems straightforward yet the distinction is very profound. Cyber threats are becoming more sophisticated, making early detection and rapid response not just beneficial but essential for organizational survival. This integration facilitates a more nuanced, dynamic response mechanism, enhancing the effectiveness of both preventive measures and recovery strategies.

Complying with DORA and fighting ransomware and malicious insiders can be resource intensive. The situation becomes more difficult when introducing new operating systems, testing for (or receiving third-party reports about) vulnerabilities and determining strategies to counter their effects. The organization needs to continually discover variants of known malware and ransomware that are regularly being developed. Ransomware is big business, and DORA helps strengthen the EU Financial Industry. An unintended side effect of being DORA-compliant means bad actors are motivated to continue to innovate new ways to penetrate an organization's infrastructure and halt its business. Even with significant effort by system and backup administrators to protect corporate data, ransomware and malicious insiders can still occasionally get through and impact a company's most critical data. That's why having a holistic, multi-layered, comprehensive strategy is essential—and the best defense.

A Call to Action

The integration of cyber recovery solutions is not only a strategic necessity, but it will soon illicit legal action. The mission extends beyond protecting your organizations' digital assets. We must also ensure that our defense mechanisms are DORA compliant. Cybersecurity spending is predicted to exceed $1.75 trillion cumulatively from 2021 to 2025, which underscores the scale of investment in combating these threats and the importance of strategic integration within cybersecurity efforts.

Explore Veritas 360 Defense to discover how Veritas can help you control your data, increase resilience against cyberthreats, and ensure compliance. Our solutions are not just about recovery; they're about empowering your SecOps team with the tools and integrations necessary to defend against today's threats and anticipate tomorrow's challenges. Learn more about using our comprehensive solutions to build a more secure future for your data.

Using our cyber recovery checklist , you can recover with confidence, leaving zero doubt about your plan against a cyberattack. It provides a phased approach so that you know where to start and how to prioritize.

Be sure to subscribe to the Veritas Cybersecurity Newsletter on LinkedIn for insights on enterprise-grade cyber resilience. Veritas is here to help you stay current on a wide range of cyber security topics, and to bolster your knowledge in preparation for DORA to go into full effect.

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

V2115 07/24