VERITAS

DORA

Deep Dive into the Cyber Resilience Aspects of the New Legislation

Authors:

Phil Yaccino
Senior Distinguished Engineer

Petter Sveum
Senior Distinguished Engineer

Alain Pelegrin
Distinguished Engineer

Sonya Duffin
Director, Solutions Marketing

White Paper | August 2024

Executive Summary

78% of Europe's top financial institutions faced third-party breaches last year.[1] These high numbers illustrate the crisis that can't be ignored. Cybercriminals and security experts are in an arms race. Ransomware attacks are increasing in number and complexity. Our financial institutions are vulnerable; therefore, leadership is taking proactive action with new legislation.

The Digital Operational Resilience Act[2], or DORA, is the new EU legislation intended to help organizations in the financial sector improve their resilience against cyberattacks. The legislation provides a unified framework for securing information and communication technology (ICT). In summary, it is intended to ensure financial sector organizations can withstand, respond to, and recover from all types of data, communication, and technology-related disruptions and threats.

Compliance with DORA is two-fold. First organizations must prove they are cyber resilient and their posture can deliver the required digital operational resilience.Secondly, they must prove their governance framework is in place to manage risk, including ICT Risk Management and the monitoring of 3rd-Party Risk Providers. The act applies not only to financial firms but also to third parties that provide the firms with ICT systems and services.

However, that is merely a high-level summary. Today's security teams need to know the specifics — controls, processes, and reporting requirements for achieving DORA compliance and how Veritas products help enterprises in their journey to become compliant. This white paper will provide an understanding of what an enterprise needs to consider while working towards DORA compliance, from a cyber resilience perspective:

- How to understand DORA and how it applies to your enterprise.
- Map specific processes and controls to DORA requirements.
- Meet DORA requirements by securing all data across the organization, to all parts of the infrastructure (on-premises, Cloud and hybrid).
- Explore how Veritas helps organizations stay compliant and resilient.
- Non-compliance and failure to comply.

Complying with regulations like DORA is a complex endeavor. Particularly due to high penalties if found non-compliant. 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.[3]

Introduction to Veritas Cyber Resilience

At Veritas, we are in the business of helping our customers be resilient. Veritas assists enterprises to become compliant by providing leading data security and protection solutions for cyber resilience.

We enable our customers to prioritize data and applications for optimal recovery. Veritas secures the infrastructure with zero-trust principles including best practices like MFA (Multi-Factor Authentication), MPA (Multi-Person Authentication), RBAC (Role-Based Access Control), and encryption. We provide solutions for physical or virtual airgap and immutable storage to ensure data integrity and protect backup data for flawless recovery. During recovery, we scan for malware to ensure no infected data is restored. Veritas also provides industry leading anomaly detection - real-time during backups, paired with user behavior analytics (UBA) for proactive platform self-defense capabilities, with minimal performance impact.

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 and 64 total articles.

→ Regulation applies to all member states of the European Union and to all corporation that operate in those countries.

→ It 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

1. ICT Risk Management and Governance, Articles 5 - 16

   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. Noting that the ability to identify and classify all critical data is mandatory with clear documentation of dependencies required.
   - Business impact analysis is required especially around cyberattacks and disasters. Business continuity and disaster recovery plans are mandated with rules around data backup and recovery, 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/SOAR, vulnerability and patch management.

2. ICT-Related Incident Management, Articles 17 - 23

   This pillar emphasizes 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. A third and final report that analyzes the root causes of the incident.
   - Where previous reporting standards often varied between jurisdictions, leading to inefficiencies and gaps in regulatory knowledge, under DORA, all entities must adhere to standardized conventions. For instance, a payment service provider experiencing a data breach must now follow specific protocols to report the incident to regulators, ensuring timely and uniform responses across the sector.

3. Digital Operational Resilience Testing, Articles 24 - 27

   This pillar focuses on mandating rigorous testing requirements to find, fix, and reduce vulnerabilities.

   - Entities must perform vulnerability and scenario-based testing yearly.
   - Additional requirement for threat-led penetration testing (TLPT) every three years to those deemed critical to the financial system.
   - Entities must also fully address any vulnerabilities identified during tests.

4. Third-Party Risk Management, Articles 28 - 44

   In today's interconnected financial ecosystem, third-party service providers play a critical role. This pillar focuses on enhancing oversight and management of ICT third-party service providers, including cloud computing services. 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 including arrangements for clear exit strategies. Meaningful plans must be in place for how to transition 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.

5. Information Sharing, Article 45

   This pillar promotes sharing cyber threat intelligence among organizations to boost collective resilience against cyber threats. By fostering a culture of sharing information, it aims to improve the sector's readiness and response abilities.

Why Veritas?

Veritas provides solutions for the cyber resilience articles within the DORA legislation. Let's dive into each of them:

A Map to DORA's Key Cyber Resilience Articles

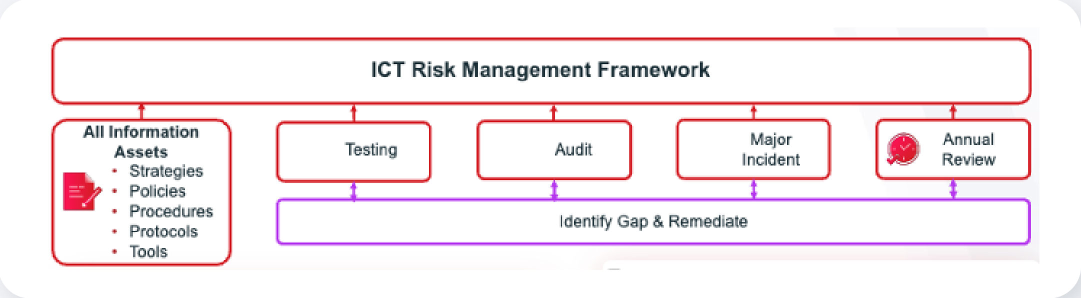
Articles: 5 Governance and Organisation, 6 ICT Risk Management Framework and 8 Identification:

Article 5 outlines the responsibilities of the management body of financial entities including:

- *Setting roles and responsibilities for ICT-related functions and establishing government arrangements*
- *Setting and approving the digital operational resilience strategy.*
- *Approving and reviewing ICT business continuity strategies, ICT internal audit plans, and the use of ICT services provided by third parties.*
- *Settling policies to ensure the maintenance of data security as well as maintain high standards of data:*
  - *Availability*
  - *Authenticity*
  - *Integrity*
  - *Confidentiality*

Article 6 lists rules ICT management frameworks requiring strategies, policies, and procedures to protect assets, including a dedicated control function. This all must be regularly reviewed and audited. Additionally, a digital resilience strategy and multi-vendor ICT strategy is a must.

Article 8 outlines that organizations should list and document their IT functions, assets, roles, and links to reduce IT risks. They must also assess cyber threats and weaknesses on a yearly basis. When network or infrastructure changes occur, they should also reevaluate risks. Financial firms should track assets, processes using third-party services, and old IT systems. They must regularly assess the risks of these elements.



How Does Veritas Help?

Veritas offers Professional Services aimed at partnering with you to help your organization get prepared. Our technology focused offerings like our Cyber Resiliency Assessment Service, offers proactive recommendations to optimize your security posture. Strategy focused offerings are focused on helping your organization set up best practices and procedures. Veritas can help you get organized and unlock the benefits of tabletop exercises. Get specialized and personalized support for your organization's needs with Veritas Business Critical Services.

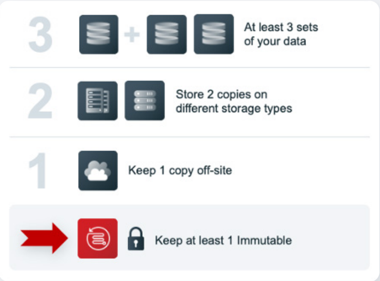
Article 9 Protection and Prevention:

Article 9 outlines steps for financial entities shall, "design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems."

This means that organizations need to establish and maintain robust security measures to protect their ICT systems, including:

- *Resilience: The ability to withstand and recover quickly from difficulties; ensuring the systems can continue to operate effectively even when under stress or after an attack.*
- *Continuity: Making sure that services can continue without interruption, even during a disaster or failure.*
- *Availability: Ensuring that systems and data are accessible when needed by authorized users.*
- *Authenticity: Verifying that data and transactions are genuine and not tampered with.*
- *Integrity: Safeguarding the accuracy and completeness of data and processing methods.*
- *Confidentiality: Protecting sensitive information from unauthorized access and disclosure.*

How Does Veritas Help?


3
At least 3 sets of your data
2
Store 2 copies on different storage types
1
Keep 1 copy off-site
Keep at least 1 Immutable

Veritas provides solutions that help you to Protect, Detect, and Recover with confidence. You can protect your 3-2-1 Backup strategy with immutable, air gapped, and isolated storage. Our solutions feature security controls, including Multi-Person Authorization (MPA), Privileged Access Management (PAM), Role-Based Access Control (RBAC), Encryption (both in flight and at rest) and other robust defenses. Veritas NetBackup can detect an attack with AI-powered Anomaly Detection and Malware scanning. Veritas will also help you to cleanly recover at scale - including setting up isolated recovery environment (IRE for forensic or clean room) or rehearse and restore to a sandbox environment without impacting the production environment. Read the Cyber Recovery Checklist for a comprehensive list of foundational security and data protection controls and best practices to ensure resilience.

Article 10 Detection:

Article 10 emphasizes the importance of detecting ICT-related incidents to ensure operational resilience of financial entities. The article outlines four focus areas: detection mechanisms, multiple layers of control, resource allocation, and data reporting service providers, that entities must implement to effectively monitor and manage ICT anomalies and cyber incidents.

Detection Mechanisms: Financial entities are required to "have in place mechanisms to promptly detect anomalous activities," including issues with ICT network performance and incidents related to ICT. They should also be able to identify potential material single points of failure and detection mechanisms must be "regularly tested to ensure their effectiveness and reliability."

Multiple Layers of Control: Detection mechanisms must support "multiple layers of control" with "alert thresholds and criteria to trigger and initiate ICT-related incident response processes." This should include automated alerts to relevant staff who are responsible for incident mitigation. This layered approach ensures that anomalies and threats are detected at various levels to provide a multilayered defense against ICT-related threats like a cyberattack.

Resource Allocation: Financial entities are also required to "devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies, and ICT-related incidents," with a particular focus on cyberattacks. This requirement ensures that financial entities are equipped with the critical tools, people, and financial resources to maintain effective monitoring and detection capabilities.

Data Reporting Service Providers: In addition to the requirements for financial entities, data reporting service providers must implement systems to "effectively check trade reports for completeness, identify omissions and obvious errors, and request re-transmission of those reports." This last requirement provides a measure of integrity and accuracy of trade data and helps to ensure operational resilience and regulatory compliance.

Article 10 of DORA sets out comprehensive requirements for detection to enhance financial entities' digital operational resilience, mitigating the risk of ICT disruptions like cyberattacks and helps ensure a stable financial system.

How Does Veritas Help?

Veritas solutions provide key tools necessary for financial institutions to meet the requirements of article 10 of DORA. Veritas industry leading anomaly and malware detection features are integrated across the autonomous data management, backup, and cyber recovery solutions enabling financial entities to protect their critical data. With advanced threat detection and response features, Veritas helps identify and mitigate risks promptly. Veritas also integrates seamlessly with an extensive ecosystem of cybersecurity partners with direct integration with popular SIEM and SOAR systems. Veritas provides detailed logging and reporting tools, facilitating regulatory audits and continuous improvement to financial institutions' cyber resiliency plans. Integrating Veritas comprehensive data protection portfolio can assist financial entities and their third parties to enhance their cyber resilience, safeguard against ICT-related disruptions and comply with article 10 of DORA.

Article 11 Response and Recovery:

Article 11 of DORA mandates that financial entities implement a robust ICT business continuity policy as part of their risk management framework. This is to ensure the continuity of critical business functions and includes "dedicated, appropriate and documented arrangements, plans, procedures and mechanisms" to handle ICT-related incidents effectively and minimize the damage and disruptions. Entities must activate response plans promptly to contain incidents, estimate impacts, and maintain effective communication with internal and external stakeholders.

Financial entities, excluding microenterprises, are required to submit their ICT response and recovery plans to independent internal audits. "Financial entities, other than microenterprises, shall include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities necessary to meet the obligations set out in Article 12." They are also required to conduct a business impact analysis (BIA) to assess potential disruptions using quantitative and qualitative criteria. Financial entities are expected to keep detailed records of activities during disruptions and report significant ICT incidents to competent authorities upon request.

These measures are designed to enhance the digital operational resilience of financial entities, ensuring they have a fully documented plan that has been tested to ensure a swift recovery and minimizes the impact of ICT incident, like cyberattacks.

How Does Veritas Help?

Veritas ensures robust ICT business continuity and effective incident response through comprehensive data protection, automated backup, and rapid recovery solutions. Veritas cyber recovery expertise and capabilities enable seamless restoration of critical business functions, minimizing downtime during a cyberattack. We also provide tools for regular testing and validation of ICT response plans through our non-disruptive recovery, rehearsal features, ensuring readiness and effectiveness of tabletop exercises. Our advanced analytics and reporting tools facilitate thorough business impact analyses, helping to identify critical functions and dependencies. Our comprehensive approach helps financial institutions maintain detailed records, streamline communications with stakeholders, and enhance their cyber recovery and resilience, aligning with the stringent requirements of article 11 of DORA. By integrating Veritas solutions, organizations can effectively manage and rapidly recover from ICT-related disruptions, to deliver business continuity and stay compliant with DORA.

Article 12 Backup Policies and Procedures, Restoration, Recovery and Methods:

"Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods…Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically."

This article also states that:

- *Backup systems must be activated without compromising security or data integrity*
- *ICT systems must be in place that allow for timely restores and have redundant ICT capacities*
- *Central securities depositories must have a secondary processing site that is located away from the primary one*
- *Microenterprises should decide if they need backup sites*
- *When restoring data, the necessary checks must. Be performed to ensure data integrity*

Article 12 is broken into seven points that cover your Backup of Primary Site (Point 1, 2, & 3), Recovery to a Secondary Site (Point 5 & 6) and Data Integrity (point 7).

How Does Veritas Help?

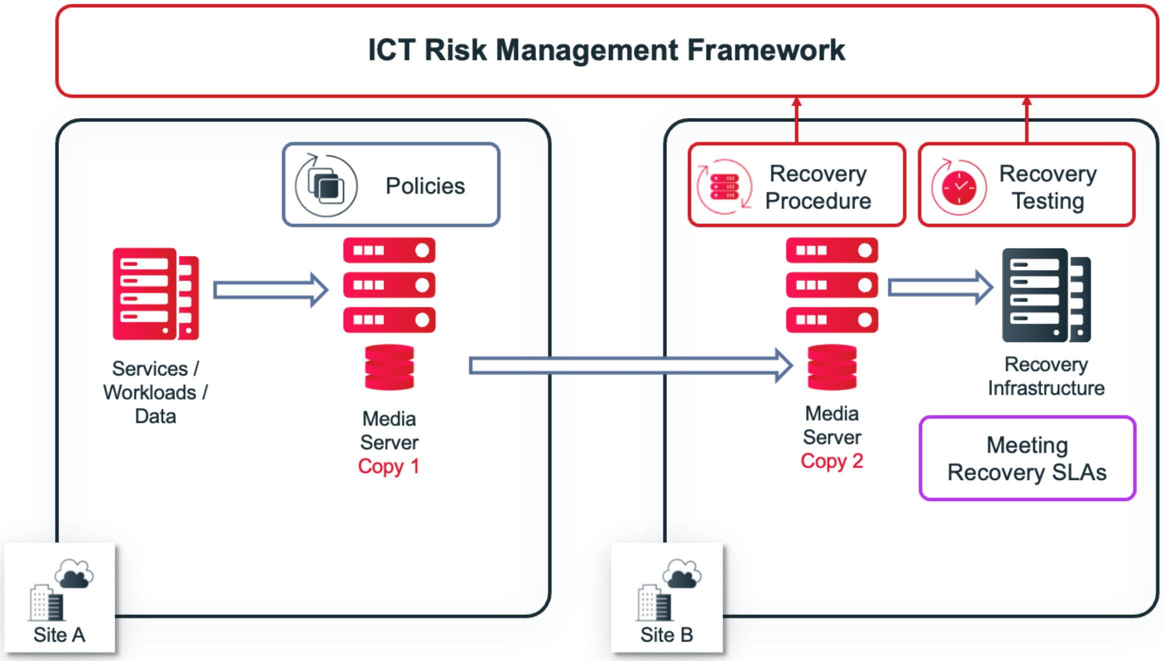
Your comprehensive solution for Article 12 is Veritas NetBackup.

Starting with how NetBackup helps you develop and document your backup policies and procedures. Including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each function. You can specify the scope of data that is subject to the backup and minimum frequency of the backup. This can be based on the criticality of information or the confidentiality level of the data. Additionally, NetBackup helps to develop and document your restoration and recovery procedures. NetBackup facilitates regular testing of the backup procedures and recovery process that is sandboxed and non-disruptive to production.

NetBackup allows for flexibility in recovery options with complete recovery orchestration to any kind of secondary site. As the legislations states your secondary site should be geographically distant and immediately accessible for critical and important functions. NetBackup allows for recovery anywhere to anywhere. Meaning that your destination data center need not be on prem or back to where the data originated, it can be stood up from self-describing data stored in a deduplicated state on the cloud providing an entire data center on demand. In addition, Alta View Orchestrated Recovery can create an on-demand recovery plan where customers can add VMware VMs & Cloud IaaS VMs (Recovery and Rehearsal workflows) into that recovery plan with pre-checks as well. Veritas allows multiple methods for replication beyond backups, to let you define and achieve aggressive Recovery Point Objectives to reduce data loss during a high impact Ransomware attack. In nutshell, Veritas lets you choose and orchestrate methods such as backup replication, I/O replication for VMs, built-in array and database replication integration.

To ensure data integrity, NetBackup helps facilitate setting up an isolated recovery environment (IRE) with a segmented clean room) that ensures the data restored is clean and safe for recovery.

- *Enables air-gapped backup copies by disconnecting network access to a secure version of your critical data, giving administrators immediate access to clean files and effectively neutralizing the effects of ransomware attacks.*
- *Pull-based replication prevents attackers from pushing data into an isolated recovery environment. It creates a virtual air gap with ingress allowed only for authorized data requested from within the isolated environment.*
- *Immutable storage provides the ability to preserve and secure data to ensure data integrity and seamless recovery.*
- *Automatic AI-powered anomaly detection and malware scanning detect and notify you before an event can occur allowing immediate action on malicious activity.*



Article 24 Digital Operational Resilience Testing:

Article 24 outlines that all financial entities must set up and rigorously test a digital operational resilience plan. It must be an integral part of the ICT risk-management framework referred to in Article 6. The approach must be risk-based and include a range of assessments, tests, methodologies, and reviews. An independent internal or external party must also conduct tests without conflicts of interest. Article 24 recommends yearly testing, and organizations must document all findings and remediation plans.

How Does Veritas Help?

Veritas partners with you via both our Professional Services and solutions to help your organization get prepared, test, and refine. Our Cyber Resiliency Assessment Service offers proactive recommendations to optimize your security posture. In addition to tabletop exercises, Veritas can help you organize and optimize your strategy with best practices and procedures. Veritas NetBackup can also facilitate a sandboxed, non-disruptive recovery rehearsal environment for testing and clean recovery.

DORA Non-Compliance

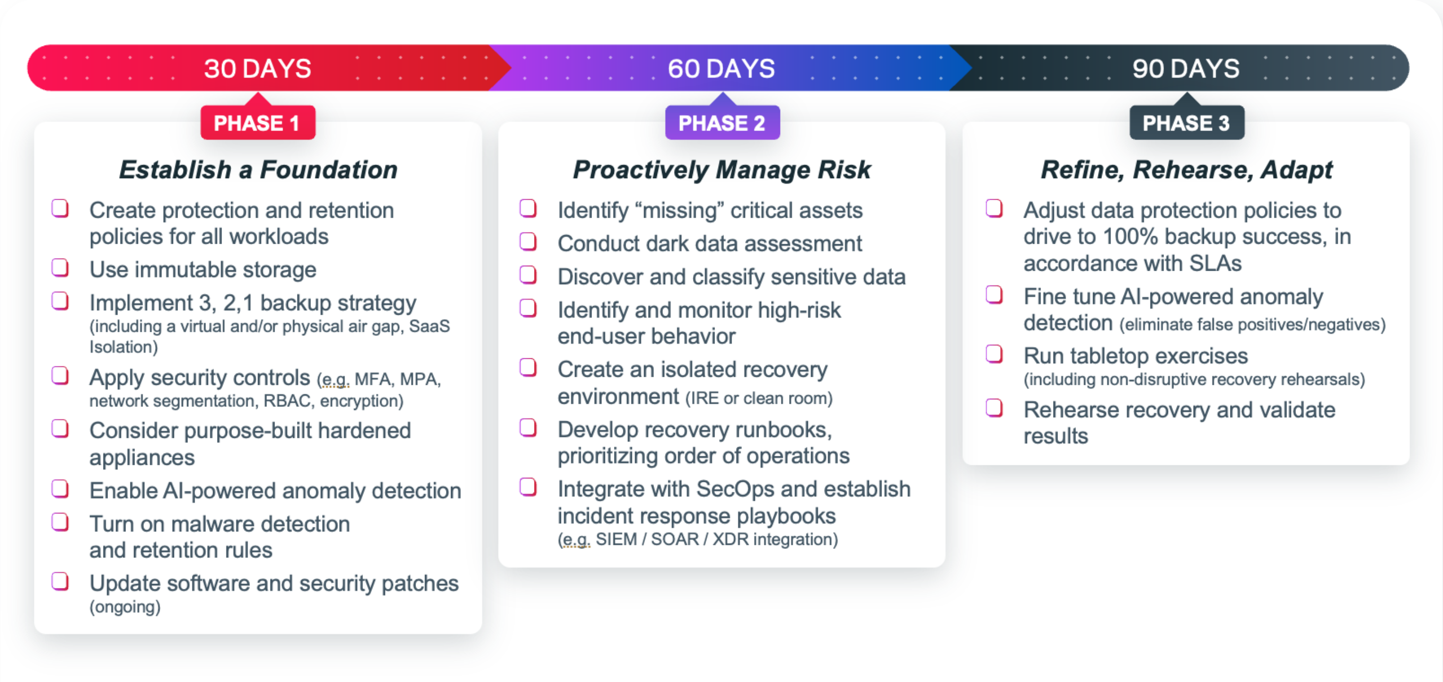
Non-compliance of the DORA Pillars is not advisable. DORA enforces strict penalties, to ensure digital operational resilience for financial institutions. Failure to comply with DORA regulations can have severe penalties. This reflects the Regulation's strict position on cyber resilience.

- 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
  A common trend around the globe, executives could be held liable for cyber incidents. Specifically, if leadership is proven to be negligent by deliberately ignoring or did not act on known risks.
- 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 from 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.

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 organizations' digital assets. We must also ensure that our defense mechanisms are DORA compliant. The solution needs to be intelligent, agile, and integrated, just as the threats the EU Financial Industry faces. Spending on cybersecurity is predicted to exceed $1.75 trillion cumulatively from 2021 to 2025. This shows the scale of investment in fighting these threats. It also shows the importance of integrating strategies within cybersecurity efforts.

At Veritas 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.



30 DAYS

PHASE 1

Establish a Foundation

□ Create protection and retention policies for all workloads
□ Use immutable storage
□ Implement 3, 2,1 backup strategy (including a virtual and/or physical air gap, SaaS Isolation)
□ Apply security controls (e.g. MFA, MPA, network segmentation, RBAC, encryption)
□ Consider purpose-built hardened appliances
□ Enable AI-powered anomaly detection
□ Turn on malware detection and retention rules
□ Update software and security patches (ongoing)

60 DAYS

PHASE 2

Proactively Manage Risk

□ Identify "missing" critical assets
□ Conduct dark data assessment
□ Discover and classify sensitive data
□ Identify and monitor high-risk end-user behavior
□ Create an isolated recovery environment (IRE or clean room)
□ Develop recovery runbooks, prioritizing order of operations
□ Integrate with SecOps and establish incident response playbooks (e.g. SIEM / SOAR / XDR integration)

90 DAYS

PHASE 3

Refine, Rehearse, Adapt

□ Adjust data protection policies to drive to 100% backup success, in accordance with SLAs
□ Fine tune AI-powered anomaly detection (eliminate false positives/negatives)
□ Run tabletop exercises (including non-disruptive recovery rehearsals)
□ Rehearse recovery and validate results

Remove doubt that you will be resilient from a cyberattack and compliant with DORA by completing the cyber recovery checklist. It provides a phased approach to Cyber Resiliency to help you know where to start and how to prioritize. The checklist outlines three clear phases to get your posture secure and resilient.

A great way to stay current on a wide range of cyber security topics is to subscribe to the Veritas Cyber Resilliency Newsletter on LinkedIn.

[1] https://fintech.global/2023/07/27/78-of-europes-top-financial-institutions-faced-third-party-breaches/

[2] https://www.veritas.com/information-center/dora

[3] https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700080542405619&p5=p&p9=58700008751471969&gclid=Cj0KCQjw8MG1BhCoARIsAHxSiQnZ0FP67Gw9BMDXndBL-JNZWu_lJqOM9DPWS-_E-xQYiN9Ii7yWxUgaAkm1EALw_wcB&gclsrc=aw.ds

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