SOLUTION BRIEF

DORA Compliance with Confidence

The Pure Storage and Commvault solution helps financial institutions address the most stringent DORA requirements.

Financial institutions have invested substantial time and resources into the design and development of infrastructure to detect, prevent, and mitigate unplanned risk events. However, the interconnectedness of the global financial industry, the frequency and complexity of cyber threats, and the sophistication of malicious actors continue to rise with each passing moment. These nefarious events pose a risk that is no longer limited to individual entities, but affects the entire financial sector, leaving all adjacent industries at risk. The mindset shift from "if" to "when" has been widely accepted and has led global regulatory bodies to introduce stringent guidance and mandates designed to ensure cyber and operational resiliency to protect the integrity of the financial industry, including the EU's Digital Operational Resilience Act (DORA), NIS 2 Directive, and APRA CPS 230.

OVERVIEW

The mandates and guidance in these regulations are far reaching and some firms may find them ambiguous, leading to a continuous cycle of education, infrastructure modernization, and strategic investment in preparation for addressing both looming threats and attesting to their cyber resilience and adherence to operational best practices. The DORA regulation introduces a detailed framework to ensure financial institutions, particularly global banks, and their third-party providers are not only prepared for unplanned events, but are capable of rapid recovery should they occur. As the sophistication of threats escalates, DORA's mandates have become increasingly urgent. Even a single, unplanned disruption to business-critical applications and data can destabilize a firm's operations and network of dependent institutions, yielding potentially irreparable damage to the firm's reputation and financial stability on a global scale.

DORA represents a strategic imperative in a world where operational resilience is a must to protect the viability of the highly interdependent financial sector and global economy. Firms that succeed in meeting and exceeding DORA requirements will not only avoid administrative and/or criminal penalties, but will gain a significant competitive advantage. In contrast, those that fall short risk putting themselves at major risk of cyber attacks and disruptions that could cripple or even bring about the demise of their business.

The critical deadline of January 17, 2025, when compliance with DORA mandates will come into full effect, is rapidly approaching, and the European Supervisory Authorities have already performed preliminary dry runs to assess the readiness of selected financial entities. Over 22,000 financial entities and ICT service providers operating within the EU will be subject to DORA. Only firms who prepare and deploy adequate technology and operational solutions will thrive in this stringent regulatory environment.

PURE STORAGE AND COMMVAULT PARTNERSHIP

Pure Storage and Commvault have a long history of collaborating to deliver unique and differentiated solutions that solve real-world challenges in securing, managing, and recovering data of all types. The combination of Commvault's industry-leading cyber resilience software and the high-performance, secure Pure Storage platform enables organizations to protect their mission critical data and applications and deliver uninterrupted services to their customers and employees in the face of growing and increasingly sophisticated ransomware and other cyber threats.

By choosing Commvault and Pure Storage, financial firms can unlock the full potential of their data, drive operational excellence, address compliance obligations, and gain a competitive edge.

THE DORA COMPLIANCE SOLUTION

Given the depth and breadth of requirements related to DORA and the various systems and solutions that financial institutions may already have in place, the Pure Storage and Commvault solution was designed from the ground up to be modular. After customers have deployed the foundational components, they can then pick and choose which additional capability they need or require. Not only is critical data secured with this approach, but if systems are breached, the applications and services can be restored within the shortest possible time frame.

Cyber Resilient Vault This logically air-gapped vault serves as the foundation for the solution. It provides an isolated, immutable repository that safeguards critical data. Connectivity to the vault is controlled from within the vault and when not in use, communication to the vault is disabled.	**Cyber Resilient Vault** • Commvault secure replication into managed, air-gapped network • Pure Storage immutable data copies with SafeMode • Data integrity checking with Commvault Cloud Threat Scan
Isolated Recovery Environments These zones are completely self-contained, isolated areas where data can be restored for forensic and application analysis, to validate data as clean before returning to production, and to continuously test cyber recovery practices for organizational readiness.	**Isolated Recovery Environments** • Validation zones for incident response and application teams • Disaster recovery zone for return to service • Air-gapped on-prem with Commvault software and Pure Storage FlashBlade and FlashArray OR On-demand, isolated cloud instances using Commvault Cleanroom Recovery
Tier 1 Rapid Recovery In the event of a cyber incident, preserving evidence should be the incident response team's first priority but restoring the service to Tier 1 applications rapidly is equally important. That is why restoring to a secondary site, either on prem or in the cloud, is critically important.	**Production Rapid Restore** • Enhanced operational recovery with Pure Storage • Primary backup immutability with SafeMode Snapshots • Improved data transfer into Cyber Resilient Vault
Tier 0 Mission Critical, Ultra-Short RTO Recovery For the critical systems (e.g. Payments) the only way to achieve the most stringent recovery time objectives required by operational resilience regulations is to recover using storage-based snapshots.	**Immutable Snapshot Recovery** • Pure Storage FlashArray™ Snapshots on primary storage for ultra-short RTO • Application consistency with Commvault IntelliSnap • Secure, efficient replication into Cyber Resilient Vault

Fig 1: The Pure Storage and Commvault solution helps customers recover from cyber attacks with confidence

SOLUTION OUTCOMES

The Pure Storage and Commvault DORA compliance solution helps organizations become more cyber resilient while addressing two major categories of the technical standards outlined by DORA.

ICT Risk Management

The joint solution outlined in this document helps identify, manage, and reduce risk across information and communication technology (ICT). This includes helping to address the following DORA Chapter II Articles:

Protection and Prevention

- Built on zero-trust principles with advanced authentication, encryption, and compliance locks
- Layers of immutability, including SafeMode™ Snapshots, provide recoverability and protection against cyber threats.

Detection

- Discover and remediate risk and detect threats with risk scanning, AI-assisted anomaly detection, and cyber deception technology.
- Commvault early warnings allow organizations to coordinate response and accelerate recovery.

Response and Recovery

- Meet stringent RTOs required by regulations with storage-based snapshots.
- Commvault integrates with Pure Storage to provide rapid recovery of mission-critical systems from immutable snapshots

Resilience Testing

- Meet operational resilience testing requirements with automated, continuous cyber recovery testing

- **Article 8—Identification:** The solution provides financial entities the ability to easily identify and classify sensitive and at-risk data.
- **Article 9—Protection and prevention**: The solution is built on zero trust principles with MFA, MPA, PAM, SAML, RBAC, and granular security controls. It provides encrypted, immutable data copies for data security and protection while helping to prevent data leakage.
- **Article 10—Detection:** The solution provides AI-assisted proactive threat detection that recognizes and alerts on anomalous behavior. It also contains active threat-hunting capabilities using decoy devices to further identify suspicious behavior.
- **Article 11—Response and recovery:** The solution enables proven fast, flexible recovery of clean data including moving to isolated recovery environments and cleanrooms as part of readiness testing exercises.
- **Article 12—Backup policies and procedures and restoration and recovery procedures and methods:** The solution delivers comprehensive, best-in-class data backup with flexible configuration options, automated policy enforcement, the ability to meet various RTO and RPO objectives, integrated integrity checks, and the ability to easily and frequently test systems in isolated environments or cleanrooms.

Digital Operational Resilience Testing

The solution also helps address the resilience testing requirements outlined in Chapter IV, Articles 24-26 related to digital operational resilience testing. To address these requirements Commvault and Pure Storage deliver automated, continuous cyber recovery testing so organizations can enhance recovery processes and readiness for breaches or outages. Whether testing is conducted on-demand in cloud-isolated tenants via Commvault's Cleanroom Recovery solution or within isolated recovery environments with Commvault software and Pure Storage FlashArray™ or FlashBlade® systems, organizations can easily deliver rapid, frictionless recovery of clean data to isolated environments.

GLOBAL OPERATIONAL RESILIENCE

While initially focused on addressing upcoming European financial sector DORA regulations, the principles of operational resilience are universally applicable across all industries. Governments worldwide recognize this importance and are actively developing or implementing regulations to ensure business continuity and resilience for critical sectors, including health care, communications, energy and more.

Commvault and Pure Storage are dedicated to providing a globally scalable solution that empowers organizations to achieve digital operational resilience. By combining our expertise in data management, innovative data platform technology, and deep infrastructure understanding, we offer a comprehensive approach to protecting, recovering, and maximizing the value of your data, even in the face of disruptions.

ADDITIONAL RESOURCES

- Learn more about Strengthening Operational Resilience in Financial Services.
- Read more about Commvault's cyber readiness and recovery solutions.
- Find out more about the Pure Storage and Commvault partnership.