PURESTORAGE®

Commvault®

SOLUTION BRIEF

DORA Compliance with Confidence

Learn how Pure Storage and Commvault help financial institutions meet the most stringent compliance requirements.

Financial institutions have invested substantial time and money into the design and development of infrastructure to detect, prevent, and mitigate unplanned risk events. However, rising cyberattacks by sophisticated actors in these complex, interdependent data environments call for heightened vigilance and a more agile approach. The Digital Operational Resilience Act (DORA) reflects the reality broadly accepted by cybersecurity professionals that it is no longer a question of "if" a cyberattack will occur, but "when"—and whether you are ready.

Pure Storage® and Commvault® bring together robust capabilities to help financial institutions defend themselves against cyber threats and comply with DORA's stringent data resilience guidelines and detailed regulatory framework. Optimized for performance, reliability and scale, IT and security teams gain refined control over how they protect and recover data while radically simplifying their data resilience operations.

Cyber Resilience Is Not Negotiable under DORA

DORA regulations provide detailed guidelines and a regulatory framework to ensure financial institutions are prepared for unplanned disruptions to their IT systems and can quickly restore services should they occur. It applies to a broad spectrum of financial services organizations beyond traditional banks and credit institutions, including third-party information and communication technology (ICT) service providers.

Protection and Prevention

Built on zero-trust principles with advanced authentication, encryption, and compliance locks and layers of immutability.

Detection

Find and remediate risk and detect threats with risk scanning, AI-assisted anomaly detection, and cyber deception technology.

Response and Recovery

Address stringent regulator-required RTOs with storage-based snapshots and get rapid recovery of mission-critical systems.

Resilience Testing

Address operational resilience testing requirements with automated, continuous cyber recovery testing.

The mandates represent a call to action for companies to be proactive in their data readiness, recovery, and resilience capabilities—or face the consequences. A single data breach can cripple a financial institution's operations with recovery times averaging 21 days and an average cost of unplanned downtime of $14,000 per minute.1 It also elevates cyber risks for the interdependent network of financial entities within which it operates. Noncompliance can result in severe financial penalties for the organization, criminal charges for its administrators, and public disclosure requirements that damage brand reputation and stakeholders' trust.

Gain an Edge on Evolving Compliance Requirements

Organizations that strategically invest in building core data protection and recovery capabilities to address DORA are also strengthening their ability to address other resilience regulations such as PSD2, NIS2, APRA CPS 230, and the upcoming 2026 European Cyber Resilience Act. Equally important, they are establishing a resilient foundation for data management and storage that can become a lasting competitive advantage. Organizations that delay may find themselves falling further behind competitors. They may not be able to demonstrate their resilience to address evolving requirements and face mounting challenges in delivering the agility modern business environments require.

Address DORA Requirements with Confidence

The Pure Storage and Commvault joint solution enhances cyber resilience and addresses DORA's technical standards for managing and recovering from disruptions, as outlined in Chapter II and Chapter IV (see Appendix).

To address risk management requirements, the solution integrates Commvault's cyber resilience software with the Pure Storage secure, high-performance platform, so that financial services organizations can protect and recover critical data and applications, addressng strict recovery time objectives (RTOs) and ensuring uninterrupted services. The solution offers flexible restoration to secondary sites whether on-premises or in the cloud, using advanced automation to streamline response when it matters most.

To address resilience testing requirements, Commvault and Pure Storage provide automated, continuous cyber recovery testing. This includes on-demand testing in cloud-isolated tenants via Commvault's Cleanroom Recovery™ or within isolated recovery environments using Commvault Cloud software and Pure Storage FlashArray™ or FlashBlade® systems, enabling rapid and seamless recovery of clean data.

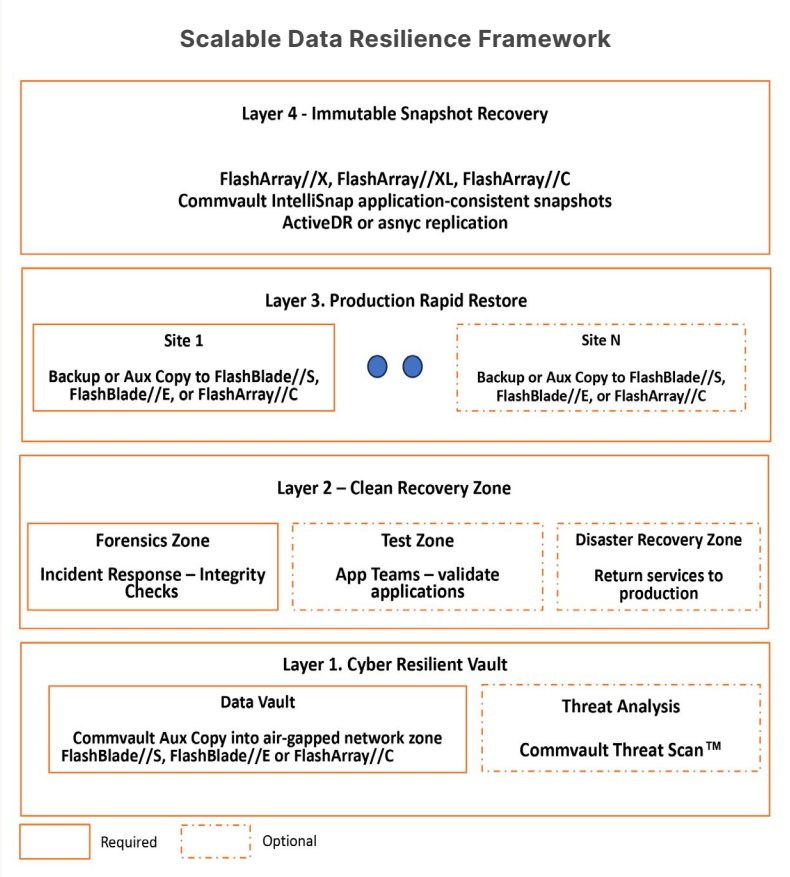
A Solution Designed for Flexibility and Scale

Given the depth and breadth of requirements related to DORA and the various systems, solutions, and infrastructure that financial institutions may already have in place, the Pure Storage and Commvault solution was designed from the ground up to be modular and highly scalable. Once foundational capabilities are deployed, financial institutions can scale up or out to address new requirements and add capabilities as needed to protect, recover, and test resilience for data of all types, simply and cost-effectively.

The comprehensive Pure Storage and Commvault solution has four layers. Each layer is a combination of technologies that address a specific outcome for enhanced data resilience.

Layer 1: Cyber Resilient Vault to Safeguard Backups

The logically air-gapped Cyber Resilient Vault is the required foundation for the solution. It provides an isolated, immutable repository that safeguards critical data. The Data Vault controls are isolated from the customer production environment to reduce the risk of credential leak and unauthorized access. When not enabled for data replication, communication with the production system is disabled. Commvault Threat Scan™ also resides in this zone to run additional scans of the replicated production backup data that was previously scanned in the customer's production datacenter, enabling a clean copy to be recovered in the Clean Recovery Zone.



Layer 2: Clean Recovery Zone to Recover and Test Applications

The Commvault and Pure Storage solution decouples necessary forensic analysis of an infected production environment from the execution of recovery operations, such as restoring business critical applications. This is accomplished using an on-premises, air-gapped isolated recovery environment (IRE) solution. The IRE can work in conjunction with on-demand public cloud tenants offered by Commvault Cloud Cleanroom Recovery.

Layer 3: Production Rapid Restore to Speed and Simplify Data Transfer

Pure Storage FlashBlade immutable object storage serves as the target for Commvault Cloud backups. High-performance FlashBlade enables fast, secure, and reliable restores of the largest data sets to address regulatory recovery targets for production services set forth in DORA. Enable immutability with S3 Object Lock, and once back up data is written, it cannot be altered or deleted, providing additional layered security.

Layer 4: Immutable Snapshot Recovery on Premises or in the Cloud

In the event of a cyber incident, preserving evidence should be the incident response team's priority. However, rapidly restoring service to Tier 1 applications is equally important. That is why restoring to a secondary site, either on premises or in the cloud, is critically important.

For critical systems such as payments, the only way to achieve the most stringent recovery time objectives required by operational resiliency regulations such as DORA, is to use storage-based snapshots. With Pure Storage FlashArray, replicated snapshot data can be used for fast, seamless recovery of systems while SafeMode™ provides an added layer of immutability so that data is available and consistent in the event you need it.

Global Operational Resilience

The principles of operational resilience are universally applicable across industries. Governments worldwide recognize their importance and are actively developing or implementing regulations to ensure business continuity and resilience for critical sectors. Working with Commvault and Pure Storage, any organization can move more confidently to address today's and tomorrow's data resilience requirements and protect the value of your data, even in the face of disruptions.

The Pure Storage and Commvault Partnership

Pure Storage and Commvault have partnered since 2010 to 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 increasingly complex and sophisticated 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.

Additional Resources

- Learn more about strengthening operational resilience in financial services.
- Find out more about the Pure Storage and Commvault partnership.
- Read more about Commvault's cyber readiness and recovery solutions.

1 | 2024 Ransomware Attack Statistics & Trends to Know, October 22, 2024

Appendix

The below table outlines DORA Chapter II Articles for ICT Risk Management and the Digital Operational Resilience Testing requirements outlined in Chapter II, Articles 8-12 and Chapter IV, Articles 25-26.

DORA Article Description	Pure Storage Capability	Commvault Capability
Chapter II – Articles 8-12		
Article 8 – Identification Identify, Classify and document all ICT functions. Identify critical systems and data and document 3rd party providers	Pure Storage FlashArray and FlashBlade integrate with Pure1™ AI-driven analytics to enhance data classification, ensuring rapid identification of critical data and security status of the fleet.	Commvault Cloud Risk Analysis continuously scans and classifies data in both live and backup environments, providing searchability for critical or sensitive data as it changes. It enables data governance teams to discover, classify, and control information (data) assets through policies that govern access, retention, and deletion.
Article 9 – Protection and Prevention Organizations need to adequately protect ICT systems, ensuring they are secure and cannot be corrupted or data leaked	Pure Storage SafeMode Snapshots create immutable, encrypted backups that prevent data corruption and extend retention times so that company SLAs are met. Zero-trust architecture with RBAC and multi-layered, always-on, 256-AES encryption further strengthens security.	The Commvault and Pure Storage solution is built on zero-trust principles and enables organizations to build a cyber recovery program that includes a Security Posture dashboard, and platform-wide MFA, MPA, PAM, SAML, and RBAC with granular security. This platform provides secure, encrypted, and immutable backup copies meeting with best-in-class encryption standards. Threat Scan automatically scans live and backup data for malware threats. If malware is found, it is automatically isolated and removed from recovery actions. Commvault's Threatwise solution provides a unique cyber deception capability to rapidly identify suspicious activities that could lead to data leakage or breach. Actions can be orchestrated, and intelligence shared via SIEM and SOAR integrations.
Article 10 – Detection Organizations need capabilities to rapidly detect anomalous activities	Pure1 AI-driven analytics with anomaly detection enables real-time threat identification.	Commvault Cloud Threat Scan and Threatwise allows financial institutions to proactively detect anomalies and enhance prompt identification and response. Can be integrated into existing security and reporting solutions or standalone.

Article 11 – Response and Recovery Organizations are required to have documented ICT BC Policies with a response and recovery process. This process needs to be tested.	Pure Storage FlashArray and FlashBlade ensure rapid, policy-driven recovery via immutable snapshots and secure replication. Commvault integration with Pure ensures repeatable validation testing and fastest time to recovery.	Commvault Cloud provides a flexible and proven automated recovery process that orchestrates a recovery playbook, including the ability to recover to a cleanroom with an air-gapped copy. Automated cleanroom facilitates simplified recovery testing with low-impact and cost. Commvault also provides capabilities for continuous cyber recovery testing in isolated environments, allowing organizations to regularly assess their resilience against cyber threats and rapidly recover critical data in the event of a breach, or via on-demand public cloud tenant through "Cleanroom Recovery." This enables testing in a secure, isolated cloud environment, addressing the DORA requirement for ongoing operational resilience testing; this is often done in partnership with storage providers like Pure Storage to provide additional isolation and data protection layers.
Article 12 – Backup, Restoration and Recovery		
12.1 **Backup Policies and Procedures:** *This section outlines the need for documented policies. These policies should specify:* ** What data gets backed up* ** How often backups occur (based on criticality/ confidentiality)*	Pure Storage FlashBlade integrates with Commvault backup policies to enable frequent, policy-driven snapshots with SafeMode immutability. Automated backup validation ensures data integrity.	Commvault Backup and Recovery capabilities enable rapid recovery of data to and from multiple locations, data centers, or clouds to address RTO and RPO objectives. Threat Scan delivers clean data recovery by actively scanning data and preventing corrupted or malware-compromised data from being restored in the recovery process. Commvault Cloud backs up data assets as well as ICT assets like VMs and applications. These backups can be stored in immutable, indelible air-gapped storage to prevent tampering. Threat Scan actively scans data and VMs to detect and isolate malicious data and systems, preventing them from being restored and reinfecting recovery environments.
12.2 **Backup Systems and Testing:** *Financial entities must establish functional backup systems based on documented policies.* ** Backup system activation should not compromise security.* ** Regular testing of backups and restoration procedures is required.*	Pure Storage FlashBlade provides extremely scalable backup repositories with centralized, automatic security and immutability status. Commvault and Pure integration provides seamless failover testing.	Commvault Cloud provides robust capabilities for continuous operational resilience testing in order to demonstrate resilience against cyberthreats. The solution enables organizations to rapidly recover critical systems in an Isolated Recovery Environments (IRE) on-premises or via an on demand public cloud tenant with Commvault Cloud Cleanroom Recovery. The IRE and Cleanroom Recovery options allow customers to simulate cyberattacks and continuously assess data readiness and cyber recovery operations while safeguarding sensitive data, using a secure, integrated platform. Commvault Cloud backs up data assets as well as ICT assets like VMs and applications. These backups can be stored in immutable, indelible air-gapped storage to prevent tampering. Threat Scan actively scans data and VMs to detect and isolates malicious data and systems, preventing them from being restored and reinfecting recovery environments.

12.3 **Physically Separate Restoration Environment:** *When restoring data using their own systems, institutions need a physically and logically separate environment.* ** This environment should be secure from unauthorized access or corruption.* ** It should allow for timely restoration of services.*	Pure Storage provides a single, simplified interface for configuring its entire product portfolio with centralized observability to ensure configurations are correct and conform to the isolation requirements.	Commvault Cloud addresses this with an on-premises air-gapped IRE solution, or via an on demand, air-gapped, public cloud tenant through air gapped Cleanroom Recovery, both give customers options where data can be restored for forensic and application analysis, and eventually returned to production service.
12.4 **Redundant ICT Capacity:** ** Financial entities (except micro-enterprises) must maintain redundant ICT capacity with sufficient resources to meet business needs.*	All of the Pure Storage arrays are fully redundant and expandable and upgradable 100% non-disruptively to address any redundant ICT capacity requirements. Additionally, Pure1 provides real-time analysis of critical metrics such as capacity utilization and trending to enable any capacity requirements to be met proactively.	Automation built into Commvault Cloud solutions can help organizations use their resources more effectively and optimize their ICT capacity.
12.5 **Secondary Processing Site for CSDs:** *Central securities depositories (CSDs) need a geographically separate secondary processing site with adequate resources. This site should:* ** Have a distinct risk profile from the primary site.* ** Ensure continuity of critical functions or provide necessary services for recovery within objectives.*	Pure Storage offers a variety of replication options (sync, async, etc.) to enable a geographically distinct recovery site with high-performance access for critical recovery and forensics of impacted data.	
12.6 **Recovery Time and Point Objectives:** ** Financial entities need to define recovery time and recovery point objectives for each function.* ** These objectives should consider the function's criticality and potential impact on market efficiency. * They should ensure agreed service levels are met even in extreme scenarios.*	Pure Storage FlashArray and FlashBlade provide ultra-fast restoration via SafeMode snapshots directly and/or rapid restore integrated with Commvault. This enables organizations to address committed RTO/RPO requirements and SLAs with confidence.	Commvault Cloud provides robust data protection and recovery capabilities, including features like flexible policy management, multi-location data storage across cloud providers, automated cyber recovery testing within on-premises IRE solutions and in isolated "Cleanroom Recovery" environments. Commvault Cloud also provides advanced threat detection to enable organizations to detect and identify threats earlier and enable faster recovery of clean data in the event of a cyber incident. Addressing the requirement for continuous business operations even during disruptions; enabling them to maintain resilient data backup and recovery processes aligned with DORA's strict compliance standards.

12.7 **Data Integrity Checks During Recovery:** ** Financial entities must perform necessary checks (including multiple checks and reconciliations) to ensure the highest level of data integrity during recovery from ICT incidents.* ** These checks also apply when reconstructing data from external stakeholders for consistency across systems.*	Pure Storage arrays constantly and automatically check the integrity and health of each array and the overall fleet through AI-enabled metrics in Pure1. SafeMode ensures data consistency with automated integrity checks during recovery.	Commvault Cloud provides robust data protection capabilities, including advanced threat detection, immutable backups, rapid recovery options, and the ability to perform continuous testing in isolated environments (like "Cleanroom Recovery") which allows financial institutions to address the stringent operational resilience requirements of the regulation, including integrity checks during recovery. Commvault Cloud Threat Scan allows financial institutions to proactively detect anomalies and enhance prompt identification and response. Can be integrated into existing security and reporting solutions or standalone.
Chapter IV, Articles 25-26		
25 **Testing of ICT tools and systems**	Pure1® offers comprehensive security assessments, providing actionable insights and prioritized recommendations to address vulnerabilities. Pure Storage has achieved SOC 2 Type II compliance, demonstrating adherence to stringent standards for security, availability, confidentiality, and processing integrity. This certification involves an in-depth audit of the company's controls over an extended period. Pure Storage has established a robust Product Security and Incident Response Team (PSIRT) to investigate, respond, and proactively communicate security vulnerabilities impacting our products and cloud services.	Systems and ICT services can also be tested in a Cleanroom prior to deployment in production environments.
26 **Advanced testing of ICT tools, systems and processes based on TLPT**	Pure is FIPS 140-2 certified, NIST compliant, NIAP/Common Criteria validated, and PCI-DSS compliant. Certifications are available on Purestorage.com or under NDA for additional details. Pure has 3rd party penetration tests performed to ensure security and can be discussed under NDA.	Commvault Cloud achieved and maintains third-party certifications attesting to how our security and build processes uphold the highest standards of security, reliability, availability, and scalability, including ISO, SOC2, FedRAMP, and others viewable in our Trust Center. Proof of security testing, such as external penetration testing, is available by request.

PS2480-02-en 03/25