SOLUTION BRIEF

Using Commvault Cloud to Assist in DORA Compliance

The Digital Operational Resilience Act, or DORA, is a regulation by the European Union that focuses on improving cyber resilience in the financial sector.

DORA sets up requirements for financial institutions and related companies to ensure their systems can withstand cyberattacks and other disruptions. This helps keep the financial system stable and protects consumers.

WHAT IS RESILIENCE?

Resilience in the cybersecurity world refers to an organization's ability to bounce back from cyberattacks and other security incidents. Preventing attacks and defending against threat actors are key elements of any cyber strategy, but being prepared to respond and recover effectively is arguably more important. This is especially true as the reality of business today is that it's not a matter of if you're going to be attacked, but when, and how bad it will be.

Resilience will be a differentiator for your business as both you and others in your space will be tested daily by modern cyber attacks. If you're able to ensure business continuity and minimize downtime and data loss, this will help you remain trusted by your customers and allow you to capture the business of those who were not so prepared.

Because of this, governments and regulatory bodies around the world have codified what is required for organizations to remain a going concern and protect markets from the adverse effects of cyber attacks. DORA is just one incidence of this.

WHAT IS REQUIRED BY DORA?

Information and communication technology (ICT) has proven time and time again to present risk to businesses by exposing data and personal information of consumers when breached by attackers. While many acts and regulations are aimed at preventing attacks, DORA takes the perspective of the inevitability of an attack and focuses on what's necessary to ensure that organizations can withstand an attack and continue operating. This is especially important when it comes to foundational sectors, like financial services.

Risk management

The framework's purpose is to identify and address ICT risks. This includes things like unauthorized access, data breaches, and system outages. By proactively managing these risks, financial institutions can minimize the impact of cyber incidents.

Areas of focus:

1 Identify and inventory your assets, including data and infrastructure.

2 Implement security controls to protect assets, prevent breaches, and minimize the risk of data exfiltration or unauthorized destruction.

3 Utilize threat detection technologies that enable your security team to find anomalies in your environment and trigger remediation actions to neutralize threats.

Third-party risk management and mitigation

In addition to the risks to their business, organizations need to be resilient in the face of failures by third-parties. Today's reliance on cloud technologies and services that are under the control of others (hosting, off-shoring, consultants) mean that when systems go awry, you need to be able to recover not just your own data, but also potentially move it to another provider with services still intact. This portability is crucial as part of a resiliency strategy and should cover both the infrastructure (ensuring you can set up and run your business on another provider) but also the application- and workload-level portability (whether your apps can be quickly spun up on this new infrastructure).

Testing for recovery and restoration

By incorporating cyber recovery exercises and testing your recovery plans into your security strategy, you can proactively identify and address weaknesses before the response is needed. This proactive approach builds resilience, allowing your organization to weather the storm of cyberattacks and emerge stronger.

The uniqueness of every organization's infrastructure and data architecture also means that there's no one-size-fits-all approach or template that you can use to ensure resilience. One thing is for certain, though—if you don't fully practice or test a plan before it's needed during a breach, you will find out the hard way where there are gaps.

There are several ways to run tests against your cyber recovery plans:

Tabletop exercises

Simulate a cyberattack scenario using a mock environment to practice communication, decision-making, and response protocols.

Cleanroom recovery

This creates a safe, isolated space to test recovery procedures without risking re-infection of your production systems. You can recover data and applications here and see if they function as intended.

Walkthroughs or audits

Step through plans without actually recovering anything. This helps identify gaps and areas needing clarification.

Incident response, management, & handling

Modern cyber incidents require far more than just your own internal systems, people, and processes. Requirements to document and disclose breaches are plenty (GDPR, CCPA, and recent rules put in place for public companies listed on US stock exchanges by the SEC, to name a few).

Because of these requirements, organizations need to have a robust program in place to both handle their internal response, but also provide auditability by third-parties and allow management to adequately disclose a cyber incident.

Maintaining even compromised data in a clean environment allows for things like forensic analysis and reporting of how an incident unfolded, what data was affected, and the tactics, techniques, and procedures (TTPs) of the attacker. This is becoming a key issue for cyber insurers as well, as they want to see exactly what happened to determine whether a claim is payable under their policies.

COMMVAULT CLOUD FOR CYBER RESILIENCE

Commvault is the gold standard in cyber resilience, leading the charge to protect the world against ransomware and other cyber threats by helping companies reduce risk, minimize downtime, and control costs. It's the cyber resilience platform built for the hybrid world, offering the best data security for all workloads, anywhere combined with rapid, enterprise-scale recovery.

Understand and reduce risks to your data

With Commvault Risk Analysis organizations can effortlessly secure and defend sensitive data across their entire infrastructure. They gain visibility into data risks to easily identify and categorize sensitive data to collaborate with ease and mitigate potential data breaches, all while saving costs through smart proactive data management strategies.

Unstructured data can also be scanned with Commvault Threat Scan, allowing operations teams to take control and defend their backup data by proactively identifying malware threats to reduce reinfection during recovery. Threat Scan analyzes backup data to find encrypted or corrupted files so users can quickly recover trusted versions of their data.

Detect threats and anomalies to your environment

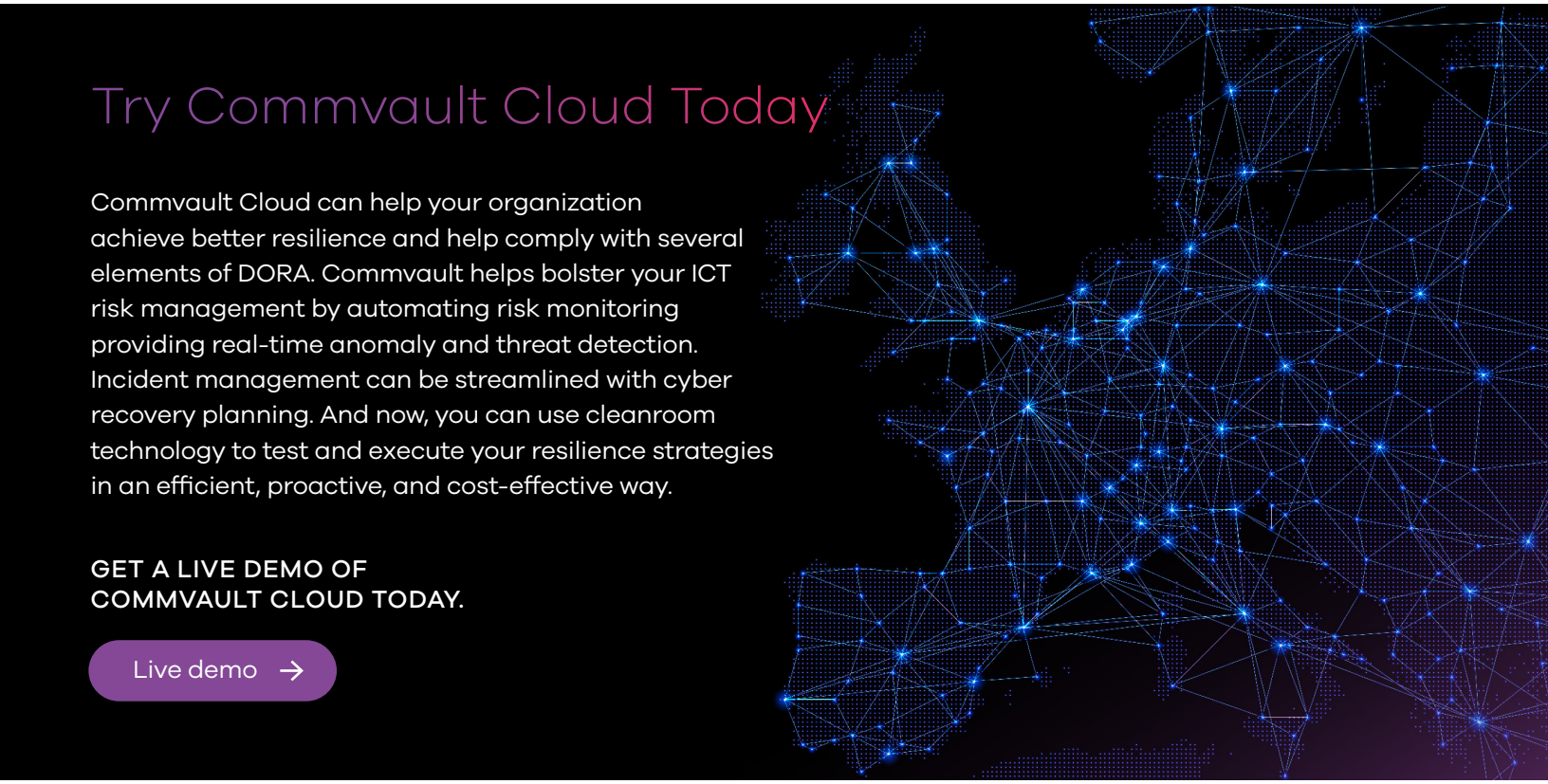
Because Commvault Cloud already backs up your data, we have the ability to intelligently detect threats to that data. The Commvault Cloud platform can look for early warnings of suspicious activity using machine learning, analyzing event timelines and establishing baseline behavior for each machine. By comparing file characteristic changes against established baselines, abnormal behaviors are identified and alerted to. This empowers administrators to take immediate action and mitigate risk.

In addition to looking at individual files for anomalies and changes, Commvault Threatwise can help surface attackers by utilizing decoys. These decoys are designed to closely mimic appealing targets for attackers who may be performing reconnaissance on your environment. They are invisible to legitimate users, but incredibly appealing to an attacker. Once an attacker engages with one of these traps, Commvault can immediately trigger high-fidelity alerts to security teams, while preserving the threat actors' interactions for forensic investigation.

Test your plans

Commvault® Cloud Cleanroom™ Recovery provides an affordable, clean, secure, isolated recovery environment on demand for testing cyber recovery plans, conducting secure forensic analysis, and business continuity.

Unlike all other data security offerings with offerings limited to disaster recovery and constrained by a limited set of workloads and recovery options, and unlike traditional isolated recovery environments, which are too expensive to execute regularly and have become increasingly complex to manage for most organizations, only Commvault Cloud Cleanroom Recovery offers the ability to recover workloads from AWS, Azure, GCP, OCI, and on-prem environments, to a safe, on demand cloud-isolated cleanroom. This comprehensive recovery platform lessens complexity and cost of using disparate tools and instead delivers the strongest and most reliable cyber resilience and readiness.



Try Commvault Cloud Today

Commvault Cloud can help your organization achieve better resilience and help comply with several elements of DORA. Commvault helps bolster your ICT risk management by automating risk monitoring providing real-time anomaly and threat detection. Incident management can be streamlined with cyber recovery planning. And now, you can use cleanroom technology to test and execute your resilience strategies in an efficient, proactive, and cost-effective way.

GET A LIVE DEMO OF COMMVAULT CLOUD TODAY.

Live demo →

To learn more, visit **commvault.com**