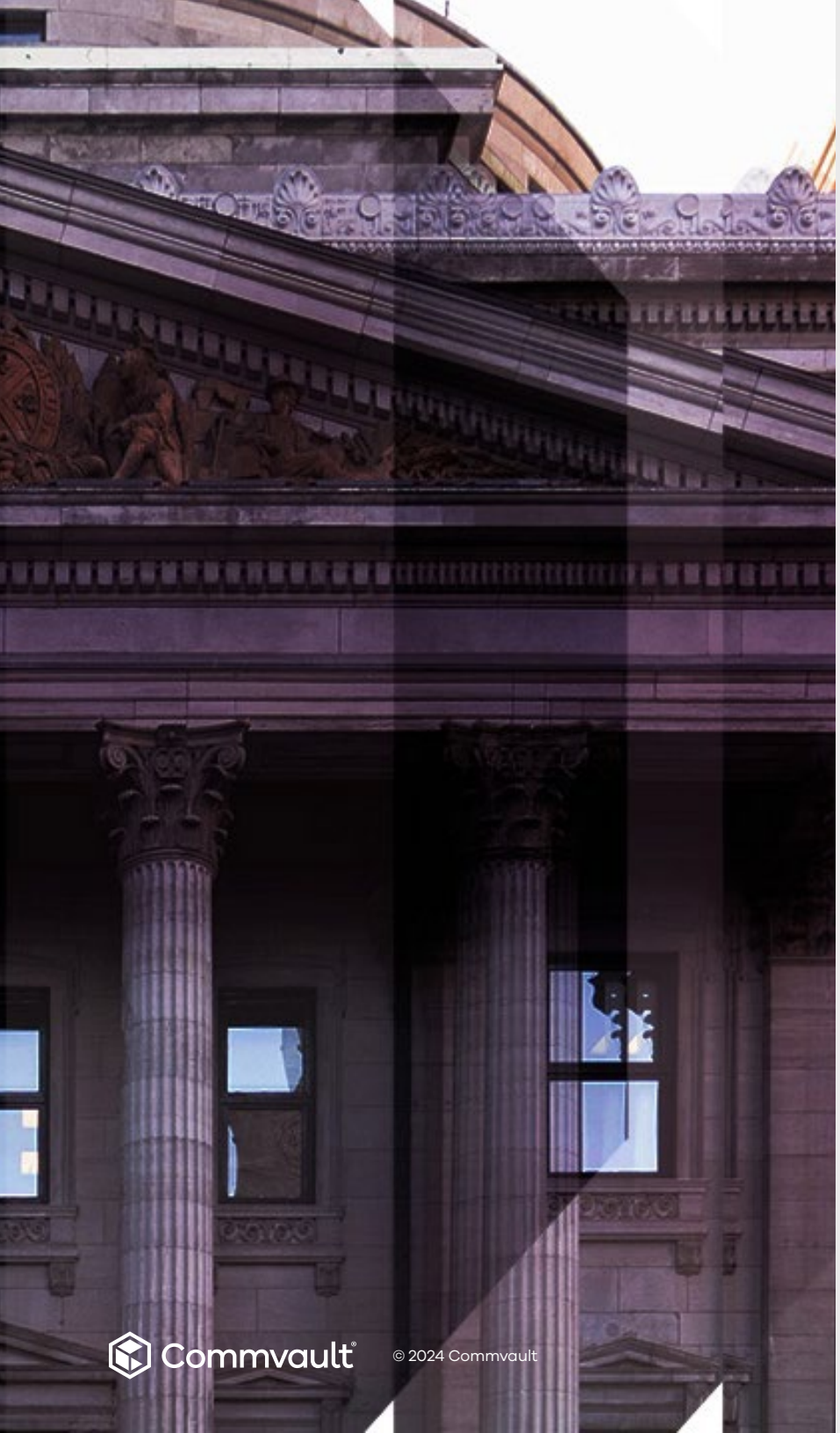
eBOOK

# Mastering DORA: Strategies for Digital Operational Resilience

## How Commvault solutions can help you navigate regulatory requirements

Commvault®

# CONTENTS







# Overview

As of January 17, 2025, financial entities in the European Union will be required to comply with the Digital Operational Resilience Act, designed to enhance cyber resiliency across the industry. It impacts banks, insurance companies, and Information and Communications Technology (ICT) third-party service providers.

## Fortunately, Commvault has solutions to help your organization supplement your compliance efforts, including:

- Identification of critical information assets to reduce risk and minimize the impact of data loss.
- Early warning of suspicious activities, integrated into existing security ecosystem.
- Secure, zero-trust, air-gapped cyber resilience recovery platform for any workload.
- Reduced complexity and cost of clean recovery and recovery testing.
- Cross-workload, cloud, and hypervisor portability to flex workloads and data between clouds or data centers.

It's crucial for all stakeholders to understand the key provisions and the impact they will have on the financial ecosystem. Let's look at the five main pillars of DORA and how Commvault solutions can help you comply with them.

# 01 Risk Management Requirements

Chapter II (Articles 5 –16) of DORA details the monitoring activities and other security procedures and policies financial institutions should establish and maintain to support a proper ICT risk management process. These policies should cover the entire lifecycle of data assets and ICT systems, from development and deployment to maintenance and decommissioning. Financial entities are expected to regularly review and update their risk management strategies to adapt to new and emerging threats.

**This means you need to:**

- Have a clear understanding of the data you have and its sensitivity as well as your assets and the potential impact of an incident on those assets.
- Increase visibility inside your network using continuous user activity monitoring.
- Analyze user activity patterns and evaluate risks by leveraging detailed audit logs and reports.
- Detect anomalies in user behavior and spot potential security risks.
- Set custom alert rules in accordance with established security policies and receive real-time notifications.

Commvault solutions can help satisfy this requirement through discovery, classifications, and protecting sensitive data; build a standardized cyber recovery platform; receive early threat warnings; divert attacks using advanced deception technology; and employ anomaly detection to aid in incident response.

Here are some specific requirements of this provision and how Commvault solutions may help:

| Provision | Commvault Solution |
|---|---|
| **Article 8 requires organizations to identify, classify, and document all ICT functions; identify critical systems and data; and document third-party providers.** | Commvault has unique capabilities to identify and classify data with Commvault Cloud Risk Analysis. This provides ICT with an automated process to keep up-to-date documentation on sensitive and critical data and act quickly. Threatwise allows for asset discovery and TTP level risk tracking when trap is exploited. |
| **In Article 9, organizations need to adequately protect ICT systems, to make sure they are secure and cannot be corrupted or data can be leaked. They are required to isolate data copies to protect from a cyberattack encrypting the data.** | Commvault allows organizations to build a zero-trust, secure cyber recovery platform with a security posture dashboard, MFA, MPA, PAM, RBAC with granular security. This single, integrated platform provides secure, encrypted, and immutable backup copies, meeting best-in-class encryption standards. |
| **Article 10 requires organizations to have capabilities to rapidly detect anomalous activities.** | Commvault Cloud® Threat Scan and Threatwise allow institutions to proactively detect anomalies in their environment, including malicious or corrupt files, large-scale changes to data, or behaviors that could indicate an attacker performing reconnaissance. Alerts about these anomalies are delivered in the Commvault platform or through integrations into existing security and reporting tools like SIEM, SOAR, or ticketing systems. |
| **Article 11 requires organizations to have documented ICT BC Policies with a response and recovery process. This needs to be tested.** | Commvault Cloud provides flexible and automated recovery processes, including the ability to recover to a cleanroom with an air-gapped copy. Automated cleanroom facilitates simplify recovery testing with low impact and cost. |
| **Article 12 outlines backup policies and procedures and methods for continuous business. Organizations should create recovery time objectives in line with business requirements and the criticality of affected systems. Organizations need the ability to recover to a different location. And for cyber recovery, organizations must have the capability to recover to a cleanroom.** | Commvault provides the capability for flexible policy management. Commvault supports multiple locations in data centers and private/public cloud providers. This is all managed with the same platform. Commvault Threat Scan monitors malware and ensures clean recovery. Commvault provides Cleanroom Recovery, allowing recovery testing to occur in an automated fashion. |

# 02 Incident Reporting

One of the pivotal elements of DORA is the obligation for financial entities to promptly report significant cyber incidents to their respective regulatory authorities. Chapter III (Articles 17 – 23) states that applicable entities need to have the means to quickly detect, track, classify, and report ICT-related incidents as well as establish responsibilities and mitigation plans for various incident scenarios. This provision ensures that there is a timely flow of information between financial institutions and financial supervisors, which is crucial for managing systemic risks and enhancing the overall resilience of the financial sector. The act specifies the types of incidents that must be reported, the reporting timelines, and the detailed information that must be included in the reports.

**Organizations must:**

- Promptly detect ICT-related incidents by receiving instant notifications on suspicious user behavior, unauthorized access, and anomalies.
- Speed up incident response process by automating countermeasures, such as blocking users and killing processes.
- Maintain a thorough evidence trail to investigate the cause, impact, and scope of the incident and prevent similar cases in the future.
- Export user activity records in a tamper-proof file format to submit solid evidence on the incident for forensic activities.
- Inform about security incidents, demonstrate security compliance to relevant authorities by submitting well-structured and informative reports.

Commvault helps organizations comply through early warning indicators using deception technology; a cleanroom for forensics capabilities; anomaly detection and threat scanning to assist in incident management; and standardized reporting with security SIEM/SOAR integration.

Here are some specific requirements of this provision and how Commvault solutions may help:

| Provision | Commvault Solution |
|---|---|
| **Articles 17 – 23 detail the ICT incident management, harmonizing and reporting capabilities organizations must have.** | Commvault Cloud streamlines Incident Response and Threat Intelligence processes through extensive ecosystem integration capabilities. Integrations with SIEMs, XSOAR, and third-party vendors facilitate efficient correlation analysis and mitigations. |
| **Articles 17 – 23 also require that organizations speed up incident response process by automating countermeasures.** | Commvault Cloud assists in providing early warning indicators to security teams and assist meeting the requirement of responding within specified timeframes to significant incidents by utilizing cyber deception and anomaly detection. |
| **Article 10 requires organizations to have capabilities to rapidly detect anomalous activities.** | Commvault Cloud® Threat Scan and Threatwise allow institutions to proactively detect anomalies in their environment, including malicious or corrupt files, large-scale changes to data, or behaviors that could indicate an attacker performing reconnaissance. Alerts about these anomalies are delivered in the Commvault platform or through integrations into existing security and reporting tools like SIEM, SOAR, or ticketing systems. |
| **Articles 17 – 23 require organizations to inform authorities about security incidents and demonstrate cybersecurity compliance to relevant authorities by submitting well-structured and informative reports.** | Commvault Cloud provides reports based on configuration and data collected by the platform, including security posture of the platform, audit trail, protection of workloads, policies used, estimated time to recover, and other elements. In addition, this data can be used to populate external tools and portals. |



# 03 Digital Operational Resilience Testing

Chapter IV (Articles 24-27) of DORA outlines that financial organizations should assess and test their preparedness for handling ICT-related incidents at least once a year to identify and eliminate gaps in operational resilience. This includes a range of testing activities, such as vulnerability assessments, penetration testing, and scenario-based exercises. These tests are designed not only to identify vulnerabilities in ICT systems and processes, but primarily to assess the effectiveness of the entity's preventive, detection, response, and recovery capabilities.

**Financial entities must:**

- Establish, maintain, and periodically test appropriate ICT business continuity plans, notably regarding critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.
- Test the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least yearly.
- Regularly test ICT systems to assess resilience against disruptions, based on DORA's testing framework.

Commvault can help organizations meet these provisions with Cleanroom Recovery, which provides recovery testing at reduced TCO and forensics testing capabilities, as well as auditable evidence and proof of success through reporting.

Here is a specific requirement of this provision and how Commvault solutions may help:

| Provision | Commvault Solution |
|---|---|
| **Articles 24 – 27 contain regular resilience operational testing requirements, including performance, compatibility, and business continuity.** | Commvault Cloud has the unique ability to orchestrate cyber recovery testing with a cleanroom in the public cloud or on-premises. This includes an air-gapped copy of the data and recovery orchestration to a clean tenant. Cyber recovery testing also can be performed in a data center using an isolated recovery environment. |



# 04 Third-Party Risk Management

Recognizing the increasing reliance on third-party ICT service providers, Chapter V (Articles 28 – 44) of DORA lists the rules and requirements financial entities need to follow to secure cooperation with ICT service providers and properly manage third-party risks.Financial entities must conduct thorough due diligence before entering into agreements with service providers.

**These entities must:**

- Monitor the activity of third-party service providers on their organization's endpoints to ensure compliance with established policies and standards.
- Define granular access permissions for third-party providers so that they only have access to the resources and data they need.
- Enhance the security of RDP connections and swiftly detect unauthorized access to sensitive data or any other potentially malicious activity.
- Configure custom live alerts and notifications on suspicious behavior and security violations of third-party users.
- Oversee the activity of third-party providers inside your IT infrastructure with the help of detailed user activity logs.
- Manage third-party risk and not be over-reliant on third parties.
- Provide technical exit strategy, where appropriate.

Commvault can help organizations comply with the regulations through cross-workload, cloud, and hypervisor data portability.

Here is a specific requirement of this provision and how Commvault solutions may help:

| Provision | Commvault Solution |
|---|---|
| **Article 28.8 outlines how organizations need to manage third-party risk and not have overreliance on third parties. They must provide technical exit strategy where appropriate.** | Commvault's any-to-any portability provides seamless data and application migration to and from third-party providers, and can be used as an exit strategy or data migration solution. |

# 05 Information Sharing

Chapter VI (Article 45) of DORA encourages financial institutions to exchange cyber threat information and intelligence to enhance digital operational resilience in the whole sector.

**Those institutions should:**

- Capture detailed records of user activity and document security incidents to share them with regulatory bodies and other financial entities as part of incident reporting and cooperation.
- Generate comprehensive logs and reports to demonstrate adherence to cybersecurity regulatory requirements.
- Export data in a protected file format to share cybersecurity evidence.

**Commvault is able to help with those efforts through:**

- Bi-directional threat intelligence/IOC exchange using native REST APIs and third-party security integrations, allowing for intelligence enrichment and event classification/upgrade to incidents.
- Encrypted and certificate signed communication over Syslog/WebHook/API calls, allowing security logs streaming for centralized proof archival and forensics collection.
- Human- and machine-initiated actions/reconfigurations fully captured through embedded audit trails, allowing for evidence recording.

Here are some specific requirements of this provision and how Commvault solutions may help:

| Provision | Commvault Solution |
|---|---|
| **Article 45 requires financial entities to capture detailed records of user activity and document security incidents. They must generate comprehensive logs and reports to demonstrate adherence to cybersecurity regulatory requirements.** | Commvault solutions enable organizations to identify sensitive data, insecure or not enabled secure configurations, and capture these within sharable documentation sets. All user activities, including API service accounts in CV interface, are captured. In addition, Threatwise can inform security communities of actual attack TTP detail through deception technology. |
| **Article 45 also requires organizations to export data in a protected file format to share cybersecurity evidence.** | Commvault solutions allow for multiple format threat intelligence and log sharing over multiple encrypted and authenticated channels like Syslog/Webhook/RestAPIs, assuring ability to centrally collect and secure all risk-related attributes using customers' centralized tools. |



# Penalties for Noncompliance

## Noncompliance with DORA can result in significant penalties, which are crucial in maintaining the integrity and effectiveness of the act.

These can vary depending on the severity and nature of the offense. They are designed to be dissuasive and proportionate to the financial strength and size of the entity, as well as the extent of the disruption caused by noncompliance.

For minor infringements, financial entities might face warnings or reprimands. However, for more serious breaches, the penalties can include criminal and/or administrative penalties. In cases of repeated noncompliance or particularly egregious breaches, regulatory authorities have the power to impose additional sanctions. These can include the revocation of licenses, temporary bans on conducting certain business activities, or other restrictions necessary to protect the financial system.

**Contact our team** to learn more about how Commvault solutions can aid your organization in complying with DORA provisions.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®