SOLUTION BRIEF

Using Commvault Cloud to Assist in NIS2 Compliance

The Network and Information Security Directive 2 (NIS2) is a European Union law that aims to increase cybersecurity across the EU. It replaces the original NIS Directive and expands its scope to cover a wider range of sectors and entities.

Essential entities (EE) providing services in sectors such as energy, transport, health, water, digital infrastructure, and finance face stricter compliance requirements, including more frequent security assessments and incident reporting. Important entities (IE), such as manufacturing and food production, face fewer but still significant obligations.

It's important to note that although NIS2 is an EU mandate, the requirements apply to organizations that provide services or products in the EU, even if they're not based there.

NIS2 is designed to improve the cybersecurity posture of organizations and bolster the resilience of the digital infrastructure used and built by EEs and IEs across the EU. The directive came into force on January 16, 2023, with EU member states given a deadline of October 17, 2024 to write regulations into law. Organizations within scope of NIS2 should be implementing programs now to comply.

WHAT IS RESILIENCE?

Resilience in the cybersecurity world refers to an organization's ability to bounce back from cyberattacks and other security incidents. Being prepared to respond and recover from cyberattacks effectively is a critical capability for today's security and IT teams. This is even more important for organizations who build and deliver the services, products, and infrastructure that society needs to function day to day.

But resilience isn't just needed by critical businesses. If you're able to implement processes that support business continuity and minimize downtime and data loss, this can be a competitive advantage in today's fast-moving digital and cloud-first world.

The need for critical businesses to understand and improve their resilience has led governments and regulatory bodies around the world to codify what is technically required so they can protect markets and their citizens from the adverse effects of cyberattacks. NIS2 is just one incidence of this.

WHAT IS REQUIRED BY NIS2?

The NIS2 Directive mandates robust cybersecurity risk management measures designed to protect network and information systems from cyber threats and minimize the impact of incidents. Articles 21 through 25 of the Directive concretely define the requirements on the part of EE and IE organizations around their cybersecurity measures.

Article 21	Article 22	Article 23	Article 24	Article 25
Cybersecurity Risk Management Measures	Security Risk Assessments of Critical Supply Chains	Reporting Requirements	European Cybersecurity Certification Frameworks	Standardization

For the purposes of this solution brief, we will focus on Article 21 and its applicability to the technology systems in place to build cyber resilience and mitigate data and infrastructure risk.

Article 21: Cybersecurity Risk Management Measures

Article 21 of the NIS2 Directive outlines the cybersecurity risk management measures that essential and important entities must implement to protect their network and information systems. The article contains key requirements around:

- **Risk Assessment:** Regularly assess potential threats and vulnerabilities to your data and infrastructure.
- **Security Policies:** Develop and implement comprehensive information security policies and procedures.
- **Incident Handling:** Establish incident response plans to detect, respond to, and recover from security incidents.
- **Business Continuity and Disaster Recovery:** Develop and maintain plans to maintain the continuity of critical operations.

There are additional details and requirements around supply chain security, access control, encryption, security awareness and vulnerability management.

As with any regulation or law, you should consult with your legal and compliance teams to determine how best to approach NIS2. Commvault Cloud delivers capabilities that can help your organization with various requirements and enables your security and IT teams to implement processes that enable backup coverage, threat and anomaly detection, and resilience during operational, disaster, and cyber recoveries.

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 only cyber resilience platform built for the hybrid world, offering the best data security for all workloads, anywhere combined with rapid, enterprise-scale recovery.

How Commvault Cloud helps with **Risk Assessment and Security Policies**	
Commvault data protection products automate data discovery and classification, threat detection, analysis, containment and recovery from cyberattacks. This helps understand and manage data risk, illuminate threats, and close security gaps.	• Threat Scan automatically scans live and backup data to detect malware threats. If malware is found, it is automatically isolated and removed from recovery actions, preventing reinfection upon recovery. • Threatwise detects attackers performing reconnaissance in data environments via decoy traps and records any interactions for forensic analysis. • Actions can be orchestrated, and intelligence shared via SIEM and SOAR integrations. • Risk Analysis enables data governance and privacy teams to discover, classify, and control data through policies that govern access, retention, and deletion.

How Commvault Cloud helps with **Incident Handling & Incident Response**	
In the event of a disruption, compromise, or failure, Commvault enables secure recovery and reconstitution of systems to a known-safe state, including the ability to recover and rebuild data, apps, and infrastructure on-prem, in the cloud, or to a Cleanroom.	• Cleanroom Recovery is an on-demand, isolated recovery environment that can be used as a failover production environment that enables business continuity after a cyber incident. The Cleanroom is separate from the production environment and serves as a clean recovery plane. • Cloud Rewind allows organizations to backup and restore full cloud applications, including their code, infrastructure, storage, networking, and security policies.

How Commvault Cloud helps with **Business Continuity and Disaster Recovery**	
Commvault provides delivers backup, recovery, and cyber resilience capabilities that are built to enable operational, disaster, and cyber recovery. The Commvault Cloud platform's coverage of workloads across on-prem, cloud, and hybrid applications and infrastructures help satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	• Commvault Cloud backs up data, apps, and systems, such as virtual machines (VMs). 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.

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 data 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 Cloud 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, Threatwise can immediately trigger high-fidelity alerts to security teams, while preserving the threat actors' interactions for forensic investigation.

Test your resilience

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

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 Cleanroom Recovery offers the ability to recover workloads from AWS, Azure, GCP, OCI, and on-prem environments, to a safe cloud-isolated cleanroom.

The processes and automations associated with Cleanroom Recovery, together with Commvault Cloud Rewind enable recovery testing so security, IT, and CloudOps teams can practice and test recovery plans, building confidence in their resilience to cyberattacks and allowing practitioners to understand gaps and areas for improvement.

Try Commvault Cloud Today

Commvault Cloud can help your organization achieve better resilience and help comply with several elements of NIS2. Commvault helps your organization perform cybersecurity risk management measures and automate monitoring of controls. Cyber resilience capabilities such as recovery testing, backup and recovery for cloud and hybrid workloads, threat and anomaly detection, and more can serve as mechanisms to comply with requirements while helping your security and IT teams maintain continuous business.

Get a live demo today to see how Commvault Cloud enables you to test and execute your resilience strategies in an efficient, proactive, and cost-effective way.