SOLUTION BRIEF

Using Commvault Cloud to Assist in SOCI Compliance

The Australian *Security of Critical Infrastructure Act 2018* (SOCI) is a legislative framework designed to protect essential services and infrastructure from various threats, particularly cyberattacks. It mandates that entities responsible for critical infrastructure assets across 11 key sectors – including energy, water, financial services, transport, and healthcare – implement robust security measures.

The overall goal of SOCI is to keep Australia's vital infrastructure secure and operational, minimising disruptions that could have severe consequences for the nation and its economy.

WHAT IS RESILIENCE?

Resilience is the ability of an organisation to recover from cyberattacks and other cybersecurity incidents. Resilience when applied to the SOCI framework is about demonstrating that you have the capability to withstand, respond to, and recover from these cyberattacks and cybersecurity incidents.

If you're able to support continuous business and minimise downtime and data loss, this will help maintain customer trust and allow you to capture the business of those that were not so prepared.

Because of this, governments and regulatory bodies around the world have codified what is required for organisations to remain operational in the face of cyberattacks. SOCI is another in a long list of recent laws that emphasise the importance of resilience and data protection.

WHAT DOES SOCI REQUIRE?

For most organisations, focusing on the Positive Security Obligations (PSOs) is the key. Organisations deemed by the government as Systems of National Significance (SoNS) also must comply with Enhanced Cyber Security Obligations (ECSOs).

PSOs

PSOs are proactive measures that responsible entities must take to enhance the security and resilience of their critical infrastructure assets.

Register of Critical Infrastructure Assets

- Entities must identify and register their critical infrastructure assets with the Cyber and Critical Infrastructure Centre.

Risk Management Program/Critical Infrastructure Risk Management Program (CIRMP)

- Applicable entities must implement a written risk management program that addresses hazards that could impact the critical infrastructure asset, including cyber risks. This program must be regularly reviewed and updated.

Mandatory Cyber Incident Reporting

- This obligation requires entities to report cyber incidents to the Australian Cyber Security Centre (ACSC).

ECSOs

In addition to the PSOs, SoNS also much comply with ESCOs by developing and maintaining a comprehensive cyber security incident response plan to effectively manage and mitigate cyber incidents. In addition, they may be required to:

- **Conduct cyber security exercises** to test and validate incident response processes and capabilities.
- **Perform vulnerability assessments** to identify weaknesses or gaps.
- **Provide relevant system information** to the government.

Building a CIRMP

Entities required to have a CIRMP also must establish a risk management program to minimise or eliminate material risks and to mitigate and effects of any material risks to their critical infrastructure.

Building a CIRMP requires an entity to first identify and assess material risks or "hazards" that could impact the availability, integrity, reliability, and confidentiality of their assets. Once identified, the organisation must put in place systems to minimise or eliminate and mitigate any effects of the identified hazards. "Cyber and Information Security" is a specific hazard identified by SOCI.

Data breaches, ransomware, and cyberattacks can cause massive financial and reputational damage. Therefore, a robust data protection and recovery strategy is an important part of minimising, eliminating, and mitigating a Cyber and Information Security Hazard.

COMMVAULT CLOUD FOR CYBER RESILIENCE

Commvault helps organisations improve their cyber resilience; minimise downtime; control costs; and minimise, eliminate, and mitigate a Cyber and Information Security Hazard. It's the only cyber resilience platform built for the hybrid world, offering data security for the broadest range of workloads, anywhere, combined with rapid, enterprise-scale recovery.

Understand Your Data Assets

Commvault can help organisations comply with SOCI by using a variety of capabilities aimed at discovery, risk and configuration assessment, and continuous monitoring.

With Commvault Risk Analysis, organisations can effortlessly secure and help defend sensitive data across their entire infrastructure. They gain visibility into data risks, like overly permissive access to sensitive data, sensitive data being kept beyond defined retention periods, or data storage locations with large amounts of sensitive data that needs to be protected. Risk analysis automatically identifies and classifies sensitive data with pre-built and customisable terms and patterns so that access control and retention policies can be applied to reduce risk and data management costs.

Commvault Threat Scan scans unstructured data, allowing operations teams to take control and help defend their data by proactively identifying malware threats to reduce the likelihood of spread and prevent reinfection during a cyber recovery. Threat Scan analyzes backup data to find encrypted or corrupted files so users can quickly recover trusted versions of their data.

For cloud assets, Commvault Cloud Rewind can map application data and dependencies to better understand the interconnectedness between systems, apps, infrastructure, and critical data.

Detect Threats and Anomalies to Your Environment

Because Commvault Cloud already backs up your data, we can intelligently detect threats to it. The Commvault Cloud platform can look for early warnings of suspicious activity using machine learning, analysing event timelines, and establishing baseline behavior. By comparing file characteristic changes against established baselines, Commvault Cloud can identify and alert you to abnormal behaviors. This empowers users to take immediate action.

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

Assistance in Implementing and Testing Your CIRMP

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.

A thorough CIRMP should include regular testing with cybersecurity exercises. These exercises may involve tabletop simulations that may corrupt or take down the systems, and the exercise should enable you to understand what is necessary to restore the affected system to operation. Cleanroom Recovery enables these types of tests. Practicing helps refine your processes to recover and help mitigate the risk of ransomware, data corruption, and disasters.

Commvault Cloud Cleanroom Recovery offers the ability to recover data, apps, and infrastructure from AWS, Azure, GCP, OCI, and on-prem environments to a safe, on demand cloud-isolated cleanroom. This comprehensive recovery platform lessens the complexity and cost of using disparate tools and instead delivers reliable cyber resilience and readiness.

TRY COMMVAULT CLOUD TODAY

Commvault Cloud can help your organisation achieve better resilience and comply with SOCI. Commvault helps you implement your risk management program by automating risk monitoring, providing real-time anomaly and threat detection, and enabling teams to test their recovery in the face of cyberattacks and disasters. Incident management can be streamlined with cyber recovery planning. And 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.