eBOOK

A GUIDE TO THE SOCI Act

How Australia protects its critical infrastructure, and what your obligations are

Commvault®

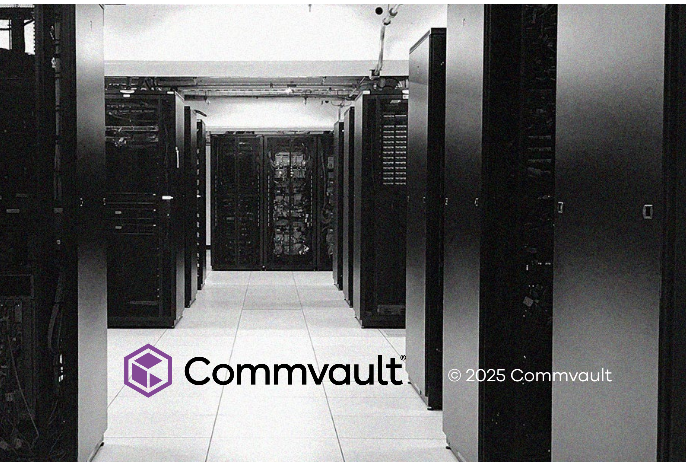
What is the Australian Security Of Critical Infrastructure Act?

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

Sectors Governed by the SOCI Act

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.

- Communications
- Financial services and markets
- Data storage or processing
- Defence industry
- Higher education and research
- Energy
- Food and grocery
- Healthcare and medical
- Space technology
- Transport
- Water and sewage



Requirements for SOCI Compliance

For most organisations, focusing on PSO is the key. Organisations deemed by the government as SoNS also must comply with ECSO.

Key acronyms for understanding SOCI

- **SOCI**: Security of Critical Infrastructure Act 2018 (Cth): A law to protect (including from cyber incidents) Australia's critical infrastructure across 11 key sectors.
- **ASD**: Australian Signals Directorate: The government agency responsible for assisting government and defence with cyber resilience and signals intelligence.
- **ACSC**: Australia Cyber Security Centre: A government agency under the ASD that is the technical authority on cybersecurity.
- **PSO**: Positive Security Obligations: Proactive security measures entities governed by SOCI must take.
- **SoNS**: Systems of National Significance: Critical infrastructure assets deemed by the government most critical.
- **ECSO**: Enhanced Cyber Security Obligations: Additional security measures that apply to SoNS.
- **CIRMP**: Critical Infrastructure Risk Management Program: A required method that applicable entities must create and implement to address hazards that could affect their critical infrastructure assets.

Positive Security Obligations

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/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

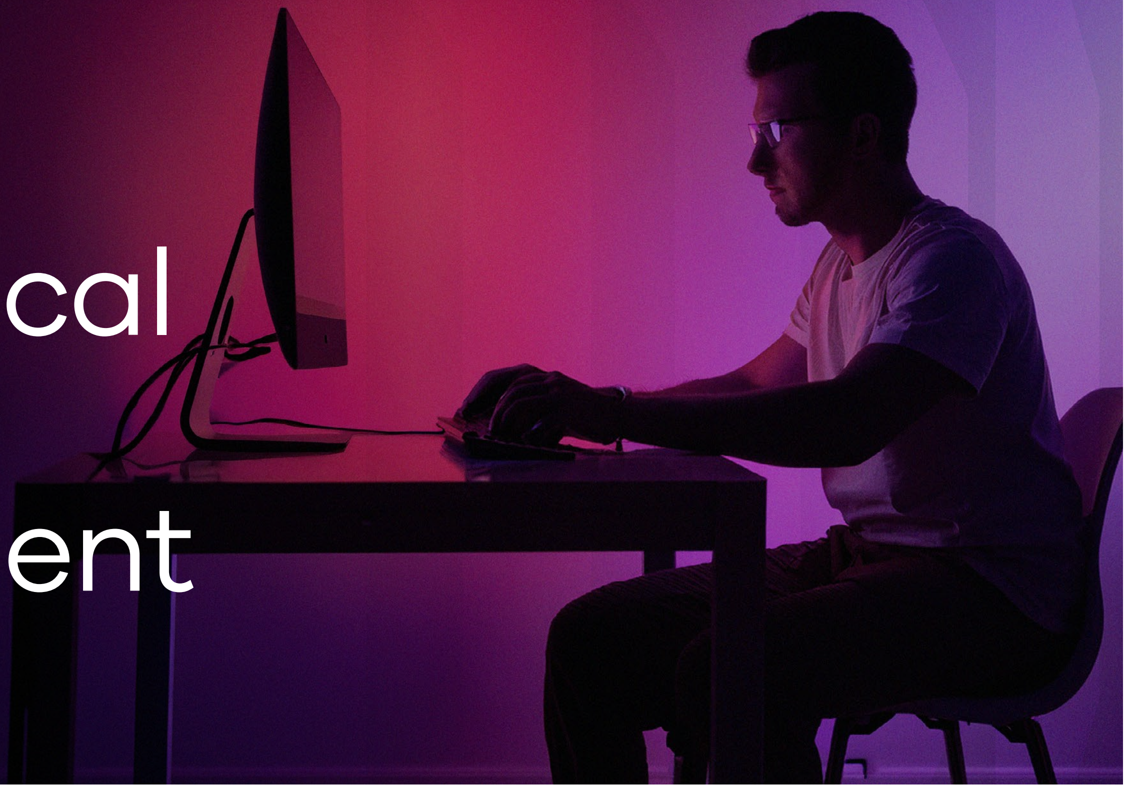
- This obligation requires entities to report cyber incidents to the ACSC.

Enhanced Cyber Security Obligations

In addition to PSO, SoNS also must 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 Critical Infrastructure Risk Management Program



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.

Testing Is Key to Building Cyber Resilience

A thorough risk management program or CIRMP should include regular testing with cybersecurity exercises. These exercises may involve tabletop simulations that corrupt or take down the systems, and the exercise should enable you to understand what is necessary to restore the affected system to operation.

Building resilience through practice

Practicing can help refine your processes to recover and help mitigate the risk of ransomware, data corruption, and disasters. A robust testing strategy will help your organisation become more resilient in the face of these attacks.

eBOOK

Help Comply with SOCI

Using Commvault Cloud

Commvault Cloud can enable your organisation to achieve better resilience and help comply with SOCI.

Commvault aids in implementing your risk management program or CIRMP 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. And thorough cyber recovery planning can streamline incident management.

Commvault Cloud enables cyber resilience with its platform-based approach to data protection, delivering data protection, backup, and recovery for organisations' workloads on-premise, and in the cloud, as well as the ability to protect and recover complex systems like Microsoft Active Directory or custom-built apps using recovery-as-code.

Cleanroom Recovery allows you to test and execute your resilience strategies in an efficient, proactive, and cost-effective way. It 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.

Contact our team to learn more about how we can help you comply with SOCI.

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