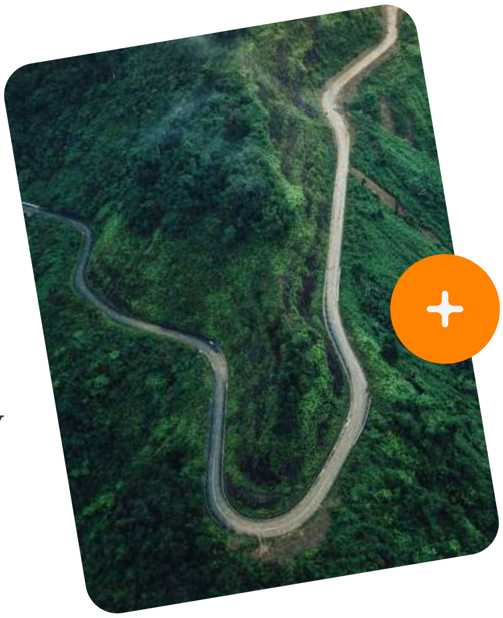
Checklist +

Introduction to the SOCI Compliance Rapid Review for Cyber Security Managers

In today's digital landscape, the security of critical infrastructure assets is paramount to safeguarding national interests, economic stability, and public safety. In Australia, the Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act) serves as a cornerstone legislation aimed at protecting essential systems across 11 vital sectors. Compliance with the SOCI Act is not only a legal requirement but a strategic imperative for large enterprises operating within these sectors.



This SOCI Compliance Rapid Review is designed to assist cybersecurity managers responsible for ensuring compliance with the SOCI Act. It outlines key considerations and actionable steps tailored to the unique requirements of the 11 essential sectors and their associated 22 critical infrastructure assets while linking to the relevant legislative documentation. Additionally, it highlights how Netskope's advanced cybersecurity solutions can support organisations in meeting their compliance obligations effectively.

From identifying critical infrastructure assets to implementing robust risk management programs and ensuring timely reporting of cybersecurity incidents, this rapid review provides a comprehensive roadmap for cybersecurity managers to navigate the complexities of SOCI compliance. This resource will assist organisations in strengthening their security posture, mitigating cyber risks, and upholding the integrity of Australia's critical infrastructure landscape.

Let's delve into the Rapid Review to ensure your organisation is prepared to meet its SOCI compliance requirements effectively.

1 Identification of Critical Infrastructure Assets (CIAs)

1A Determine if your business owns or operates any assets that may qualify as critical infrastructure assets (CIAs) within the 11 essential sectors regulated by the SOCI Act.

□ Communications

□ Data storage or processing

□ Defence

□ Energy

□ Financial services and markets

□ Food and grocery

□ Healthcare and medical

□ Higher education and research

□ Space Technology

□ Transport

□ Water and sewerage

1B Categorise your Critical Infrastructure Assets (CIAs) based on their designation as Critical Infrastructure Sector Asset (CISA), Critical Infrastructure Asset (CIA), or System of National Significance (SONS). There are 22 types and each of these are categorised differently and require different security and reporting standards.

□ Critical telecommunications asset

□ Critical broadcasting asset

□ Critical domain name system

□ Critical data storage or processing asset

□ Critical banking asset

□ Critical superannuation asset

□ Critical insurance asset

□ Critical financial market infrastructure asset

□ Critical water asset

□ Critical electricity asset

□ Critical gas asset

□ Critical energy market operator asset

□ Critical liquid fuel asset

□ Critical hospital

□ Critical education asset

□ Critical food and grocery asset

□ Critical port

□ Critical freight infrastructure asset

□ Critical freight services asset

□ Critical public transport asset

□ Critical aviation asset

□ Critical defence industry asset

How Netskope Can Help

- Netskope's private security cloud offers global coverage with 72 regions globally, ensuring visibility and monitoring capabilities across distributed environments that supports the majority of the 22 CIA's listed above.
- Utilise Netskope's data insights and analytics to discover, categorise and prioritise critical infrastructure assets, supporting compliance with their unique reporting requirements.
- Netskope DLP and introspection enables the protection of sensitive content that matches DLP profiles as defined by the organisation, specific to the 22 CIA's listed above. It also includes pre-defined DLP profiles for regulatory compliance.

2 Notification Obligations for Cybersecurity Incidents

□ Understand the notification obligations in the event of a cybersecurity incident as outlined by the Australian Signals Directorate.
Part 2B of the SOCI Act.

□ Ensure timely reporting of cybersecurity incidents within the specified 12-hour or 72-hour window.

How Netskope Can Help

- Netskope's visibility and monitoring capabilities enable real-time detection and notification of cybersecurity incidents, supporting compliance with reporting obligations within the specified window.
- Gather information from remote sites at scale and pace to facilitate timely reporting to the Australian Signals Directorate. With Patented Netskope Cloud XD™, Netskope goes deeper and understands more to quickly target and control activities across thousands of cloud (SaaS and IaaS) services and millions of websites that are used across your organisation.

3 Implementation of Critical Infrastructure Risk Management Program (CIRMP)

□ Establish a critical infrastructure risk management program (CIRMP) in accordance with legislative requirements.
Part 2 Requirements in the SOCI Act.

□ Regularly review and update the CIRMP to address evolving cyber threats and vulnerabilities.

How Netskope Can Help

Leverage Netskope's data insights and analytics to inform the organisation's CIRMP, enabling data-driven risk management decisions.

Utilise Netskope's customisable policies to align with specific cybersecurity controls mandated by the SOCI Act.

4 Consequences of Non-Compliance

□ Understand the penalties for non-compliance with the obligations outlined in the SOCI Act, including fines of up to 200 penalty units per day.
Part 5, Division 4 of the SOCI Act.

How Netskope Can Help

- Netskope provides comprehensive cybersecurity solutions to strengthen your organisation's security posture and mitigate cyber risks.
- Ensure compliance with SOCI Act requirements through Netskope's visibility, data protection, threat protection, policy enforcement, incident response, and secure web gateway capabilities.

Conclusion

By leveraging Netskope's technology and expertise, cybersecurity managers can effectively meet their compliance obligations under the Security of Critical Infrastructure Act, safeguarding critical infrastructure assets and ensuring operational resilience in the face of cyber threats. As the cloud security leader serving the world's largest and most valuable customers, we have directed significant resources to ensure that our data centres, hardware, software, and processes are secure, resilient, meet the most rigorous standards, and deliver the high-performance even our most stringent customers require.

To understand what compliance standards Netskope achieves, please visit here.

To understand how our platform protects complex cloud workloads, visit here.