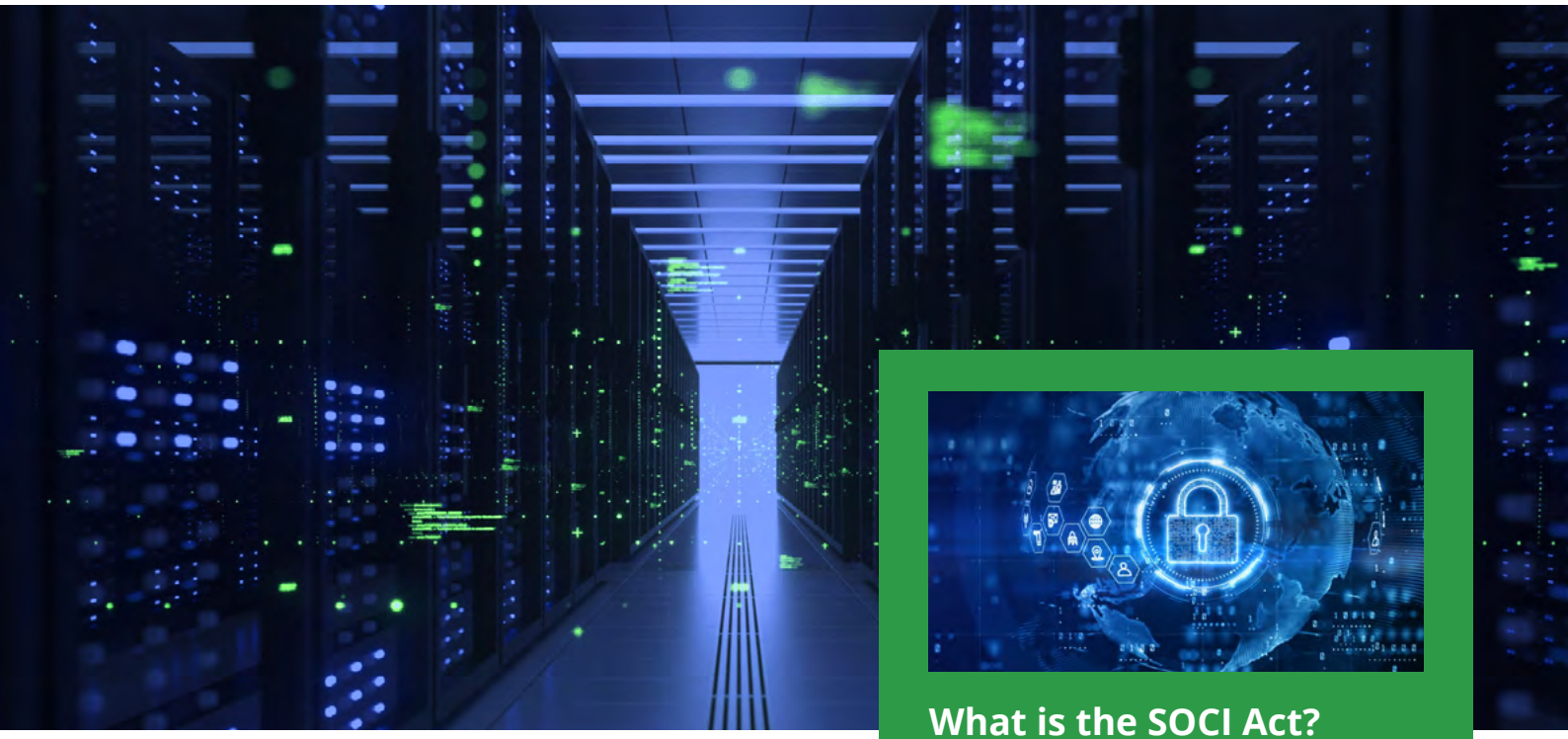
CompliantERP

SAP Silver Partner



Security Compliance and the SOCI Act: Securing Our Critical Infrastructure

Our critical infrastructure forms the backbone of modern society, providing essential services and enabling economic growth. However, this interconnected network of systems also presents a tempting target for a wide range of threat actors, from individual hackers to professional cyber criminals and rogue states. Securing critical infrastructure has never been more essential.

Here, the Security and Online Crime Investigation (SOCI) Act plays a vital role. This legislation not only bolsters the legal framework but also empowers businesses to combat cyber and physical threats. It establishes a solid foundation for addressing these threats, strengthening the trust that both individuals and businesses have in their respective systems.

With the SOCI Act in place, businesses can implement changes to their cybersecurity posture and operate with greater assurance, knowing that stringent measures are enforced to shield their critical systems from the evolving landscape of cyber threats.

What is the SOCI Act?

The Security and Online Crime Investigation (SOCI) Act, enacted in 2018, addresses the escalating risk posed by physical and cyber threats that target vital sectors like electricity, gas, water, and supply chain industries. This legislation establishes important mandates for these sectors to bolster their defences against said attacks, fortifying their overall resilience. It reflects a proactive approach to safeguarding critical infrastructure, recognising the profound implications that a breach in these areas can have on a nation's security and economy.

By imposing stringent security standards, the SOCI Act not only seeks to protect critical assets but also aims to maintain the uninterrupted functioning of essential services that underpin modern society. Every day we are reminded by the threat and impact of cyberattacks and natural disasters, and the SOCI Act is a crucial tool in the ongoing battle to secure our digital landscape and preserve the integrity of critical infrastructure.

Updates to the SOCI Act

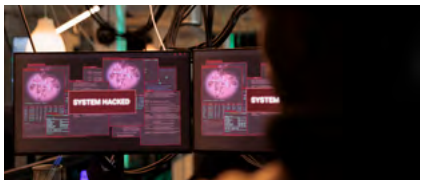
In 2021, the SOCI Act underwent significant reforms, expanding its scope from four to eleven critical infrastructure sectors, including the Data Storage and Processing sector. These reforms aim to bolster the security and resilience of critical infrastructure assets by introducing Positive Security Obligations (PSOs). The PSOs mandate that entities must proactively manage the security and resilience of their critical infrastructure assets.

Impact on the Data Storage and Processing Sector

The incorporation of the Data Storage and Processing sector into the SOCI Act has introduced significant changes, manifesting across three pivotal Public Safety Obligations (PSOs) applied to critical infrastructure assets:

Expanded Asset Information Reporting

Under the amended legislation, entities are now compelled to report in-depth information concerning the ownership and operational aspects of their critical infrastructure assets within the register of such assets. This broader scope of reporting aims to enhance transparency and accountability.



Mandatory Reporting of Cybersecurity Incidents

The SOCI Act now imposes a mandatory requirement for entities to promptly report any cybersecurity incidents they encounter. This directive ensures that incidents are swiftly identified, reported, and addressed, facilitating rapid response and mitigation strategies to minimise potential damage.

Critical Infrastructure Risk Management Program (CIRMP)

Responsible entities overseeing specific critical infrastructure assets are obligated to institute and uphold a comprehensive Critical Infrastructure Risk Management Program. This program necessitates regular reviews and updates, contributing to the ongoing security and resilience of these critical assets. The CIRMP helps in identifying and mitigating risks effectively, ultimately safeguarding the stability of critical infrastructure.

Incorporating the Data Storage and Processing sector into the SOCI Act strengthens the overall effectiveness of the SOCI Act by ensuring a more robust defence against emerging cyber threats and strengthening the protection of critical infrastructure assets.

Critical Infrastructure Risk Management Program (CIRMP)

The initiation of the Critical Infrastructure Risk Management Program (CIRMP) for designated asset classes, as outlined in the CIRMP Rules, was set in motion on February 17, 2023. A CIRMP that meets the established compliance standards is designed to aid responsible entities in effectively overseeing potential substantial risks originating from recognised hazards. This will exert a significant influence on their critical infrastructure assets. It is imperative for these responsible entities to engage in thorough efforts aimed at reducing or eradicating significant risks linked with these hazards and to counteract any detrimental impacts on the assets in question. This proactive approach not only safeguards the integrity of critical infrastructure but also bolsters the overall resilience of the systems in place.

In keeping with the principles of the CIRMP, entities must demonstrate a commitment to upholding the security and reliability of vital infrastructure components, reinforcing the foundation upon which essential services and operations rely. Through diligent risk management strategies, entities can effectively navigate potential challenges and uphold the continued functionality of critical assets, contributing to the overall safety and stability of the infrastructure landscape.

Recommendation for Businesses

Whether your business falls under the scope of applicable industries or not, the following recommendations will help bolster the cyber risk management posture of any business.

System Security Reviews

- **Vulnerability Assessment:** Conducts thorough vulnerability assessments to identify weaknesses in your critical infrastructure. By pinpointing vulnerabilities, you enable proactive remediation, reducing the risk of threats.
- **Penetration Testing:** Perform penetration tests to simulate real-world attacks on your systems. This helps uncover vulnerabilities that could be exploited and provides insights into necessary security improvements.
- **Security Patch Management:** Maintain up-to-date security patches and updates for your systems, closing potential entry points for threats.

Compliance Frameworks

- **Tailored Compliance Solutions**: Create tailored compliance frameworks to your industry's specific regulations and standards. This ensures that your critical infrastructure teams operate within a relevant and effective compliance environment.
- **Continuous Compliance Monitoring:** Implement systems for continuous compliance monitoring and threat detection, providing real-time insights into your infrastructure's compliance status.

Organisational Training

- **Customised Training Programs:** Design customised training programs to educate your staff on security best practices and compliance requirements.
- **Security Awareness Training:** Offer security awareness training to your employees to help them recognise and respond to potential threats effectively.

Audit Readiness

- **Streamlined Audit Preparation:** Streamline processes and documentation to ease the burden of audit preparation. This ensures that you are well-prepared for audits and inspections.
- **Documentation and Reporting:** Maintain detailed records and reports, making it easier to demonstrate compliance with standards and regulations during audits.

The Security and Online Crime Investigation (SOCI) Act is pivotal in strengthening essential service security. It sets rigorous standards and, with recent amendments like the inclusion of Data Storage and Processing, bolsters transparency, ensures prompt incident reporting, and enforces Critical Infrastructure Risk Management Programs (CIRMPs). These updates collectively advance a more secure and robust critical infrastructure landscape.

To address these evolving challenges, CompliantERP offers a range of solutions covering, System Security Reviews, Compliance Frameworks, Organisational Training, and Auditing Readiness. When combined, these solutions play a crucial role in preserving the integrity and stability of critical infrastructure and protecting our essential services. With CompliantERP's services, you can strengthen the resilience and security of your critical infrastructure, effectively mitigating threats and ensuring business operations while complying with the SOCI Act.

Contact us to help you progress your compliance with new SOCI Act regulations.

Phone +61 7 3217 7778
Email admin@compliantERP.com