THALES
Building a future we can all trust

Critical Infrastructure And the Role of the Board in Managing Risk

What is the SOCI Act and What Does it Mean?

Over the past several years, Australia's Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act) has undergone significant reform, expanding from four to 11 sectors and requiring captured entities to comply with enhanced cyber security obligations relating to their critical infrastructure assets.

The sectors captured by the SOCI Act span the private and public sectors, providing the services essential for everyday life, national security and economic prosperity. When it was amended in 2022, the SOCI Act was expanded on existing cyber security obligations to capture 'all hazards', capturing threats posed across physical and natural hazards, personnel and supply chains. This change was an acknowledgement of the increasing complexity of securing critical infrastructure and the multitude of events that may impact business operations. For captured entities, it also meant careful consideration of how all hazards that may impact their operations and the cascade effect they could have.

To increase oversight of critical infrastructure hazards, specific entities are now required to develop and maintain their own Critical Infrastructure Risk Management Plan (CIRMP). The CIRMP must capture the entity's critical infrastructure assets and detail the methodologies and approaches to managing risk to the assets, complimenting and augmenting existing risk and compliance management frameworks. Importantly, it must be attested to on an annual basis.

This requirement means entities must attest to the robustness of their CIRMP using retrospective data from incidents and other business events, while also attesting to its robustness over the forward-looking year.

This last point is significant, as entities must ensure they understand the evolving threat environment, analysing what it means for them and their ability to adapt and respond while maintaining operations

As a result of the introduction of the CIRMP regime, many critical infrastructure entities had to uplift existing business practices to meet the requirements in advance of the legislation going live in September 2023 and operationalisation of the first attestation in September 2024.

Through this process, captured entities are forced to consider security as much more than a 'set and forget'. Rather, they must view security maintenance and uplift as a continuous and evolving process.

Risk Management – 2025 Attestation

As organisations prepare for their 2025 attestation, the increasingly complex and dynamic risk operating environment must be considered. Some key risks include:

- Ever increasing cybersecurity threats, with foreign threat actors and sophisticated cyber criminals increasing their attacks on critical infrastructure and adjacent industries
- Data and information security risks due to the expansion of AI capabilities, including data poisoning, sophisticated phishing and credential stuffing exploits and deep fakes
- Heightened insider threat and risk of people being compromised due to their position within critical infrastructure entities
- A fractious geopolitical environment, with evolving conflicts threatening global supply chains and heightening the importance of understanding third and fourth order suppliers
- Increasing regulator oversight and enforcement of cyber security practices

These risks, while not exhaustive, illustrate the evolving and unstable environment critical infrastructure entities are operating within, underscoring the importance of robust risk management programs. Looking forward, entities should ensure they are comfortable in their ability to respond to events, in particular are rare and unpredictable 'black swan' events that may impact them directly or indirectly.

The Role of the Board

The Board plays a central role not only in the attestation process, but also throughout the year to ensure an organisation is implementing effective risk governance mechanisms and is identifying and managing all relevant risks.

Importantly, Boards should consider the operations of the enterprise risk, resilience and compliance functions of an organisation, ensuring they have sufficient investment to enable them to implement change and not simply be viewed as compliance 'tick-box'.

Tel: (03) 9880 5555 Email: info@tesserent.com Tesserent.com

THALES
Building a future we can all trust

Board Responsibilities

Boards of designated critical Infrastructure asset operators in Australia must attest to the efficacy of the risk management of critical assets by 28th September 2025, marking the second year of the RMP requirement.

The attestation is a short web-based form provided by the regulator – the Cyber and Infrastructure Security Centre (CISC) - comprising series of questions about the asset, ownership and risk management processes. While short, the form reflects the narrative of how critical infrastructure assets are managed to the regulator.

At Thales in cybersecurity, our experience indicates that completing the form takes about 15 to 30 minutes for an appropriately informed and prepared Board member. Preparation is key and it can take months to collect, analyse and present the required information for the Board. This advice is typically presented with the key artefact relevant to attestation, the CIRMP. Key to this process is the decision by the Board as to how to address questions within the form as to:

a. efficacy of risk management;

b. descriptions of realised incidents or hazards;

c. descriptions of variance to the CIRMP.

Actions to Take Now

Engagement, clear communication and collaboration are essential to ensuring Board members have the information they need to feel confident in attesting to the CIRMP. Therefore, it is vital the Board has:

- Accurate and current guidance as to the status of compliance with the SOCI Act;
- Been thoroughly briefed on the forward program for security maintenance to prepare the Board for attestation;
- Guidance on critical assets being attested to, recent incidents, the overall cyber security maturity of assets; and
- Any ongoing programs of work designed to uplift maturity or better manage risk that should be articulated in the attestation – especially in the event an incident occurred and/or cyber maturity is lower than the level expected by the regulator.

Conclusion

As we face an increasingly complex operating environment in the second half of 2025 and into 2026, organisations and their Boards must continue to think outside the box and challenge existing preconceptions.

As IT and OT continue to converge, organisations who fail to move will only have an increasingly complex and costly step gap, they will also face greater risks across the spectrum.

Therefore, the CIRMP should not simply be viewed as a compliance tool. Rather, it should empower organisations to strive for continuous risk management improvement and provide Boards with the information required to support risk management uplift programs now and into the future.

Authors

Zoe Thompson
Director - Critical Infrastructure Resilience

Mitchell Loughlan
Director - Risk & Resilience