Security of Critical Infrastructure Act

Critical Infrastructure Risk Management Program

Australian critical infrastructure entities have until 18 August 2024 to adopt and comply with a Critical Infrastructure Risk Management Program ("CIRMP") under the Security of Critical Infrastructure Act 2018 ("SOCI Act"). This legislation imposes obligations on critical infrastructure entities, with compliance activities already underway for selected assets. FTI Consulting can work with your organisation to ensure compliance with SOCI Act regulations.

KEY SOCI MILESTONES

Grace periods have ended for reporting cyber incidents, registering ownership, and meeting CIRMP obligations. Compliance is now mandatory.

18 Aug 2024

Deadline to adopt a CIRMP

28 Sept 2024

Deadline to submit Board-approved annual report to the Department of Home Affairs

2024-25 SOCI Compliance

Trial audits and compliance activities have started and are planned throughout 2024-25.

Designed to uplift Australia's critical infrastructure protection, the SOCI Act was developed to enhance cybersecurity across 11 critical infrastructure sectors. A CIRMP helps entities responsible for critical infrastructure assets establish, maintain, and comply with a risk management program. This takes a holistic and proactive approach to identifying and mitigating hazards posing material risks to availability, integrity, reliability, and confidentiality of critical assets.

The following sectors are subject to the CIRMP obligations:

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

There are four key domains within the CIRMP that entities must address:

- Cyber and information security hazards
- Personnel hazards
- Supply chain hazards
- Physical security and natural hazards

For each of these domains, responsible entities must:

- Identify material risks, where the occurrence of a hazard could have a relevant impact on the asset
- Minimise and eliminate material risks of such hazard occurring
- Mitigate the relevant impact of such a hazard on the asset

The cyber and information security domain of the CIRMP requires that critical infrastructure organisations specify how they will comply with at least one of several existing cybersecurity standards and frameworks, such as:

- Australian Standards AS ISO/IEC 27001:2015 and ISO/IEC 27001:2022;
- National Institute of Standards and Technology (NIST) Cybersecurity Framework;
- Australian Energy Sector Cyber Security Framework (AESCSF) at security profile one;
- Australian Signals Directorate's Essential Eight Maturity Model at maturity level one;
- United States of America Department of Energy's Cybersecurity Capability Maturity Model (C2M2) at maturity level one; or
- a framework equivalent to any of the above.

IN SUMMARY

Entities in scope will need to comply with the controls as defined in their CIRMP by 18 August 2024.

They will then have until 28 September 2024 to submit a Board-approved annual report to the Department of Home Affairs.

Compliance activities including trial audits have begun and are ongoing throughout 2024-25. Internal and independent audits of CIRMPs should be completed periodically.

FTI's Cybersecurity team can support SOCI preparedness and ongoing compliance.

How We Can Help

The experts at FTI Consulting will work with your organisation to define, implement, and ensure compliance with the CIRMP obligations under the SOCI Act.

Through a holistic and personalised approach, we help your organisation enhance security and resilience against the unique cybersecurity risks facing your organisation, whilst meeting your CIRMP obligations and maximising the return on investment.

Independent assessments or audits of SOCI obligations and CIRMPs can assist critical infrastructure providers to realise improvements, enabling improved risk management and asset management outcomes for critical infrastructure providers.

Why FTI Cybersecurity

Due to the complexity and interdependencies of hyperconnected digital and physical assets in critical infrastructure, the required coordination to mitigate risk and respond to incidents is a massive undertaking. Our team understands the planning required to conduct day-to-day business operations, while simultaneously preparing to implement a CIRMP. Our experts have extensive experience in industrial systems, facilities, and operational processes with deep industry expertise derived from their backgrounds in government, military, and the private sector. We have a proven track record of harmonising the technical, operational, legal, regulatory, reputational, and workforce components into workable solutions.

WOUTER VEUGELEN
Senior Managing Director
Cybersecurity
+61 2 9235 9309
wouter.veugelen@fticonsulting.com

CARLA LIEDTKE
Managing Director
Risk Management
+61 402 853 223
carla.liedtke@fticonsulting.com

LUCAS ROE
Senior Director
Cybersecurity
+61 2 8022 5708
lucas.roe@fticonsulting.com

06132024 | VN02678-v08