Security of Critical Infrastructure Act

Critical Infrastructure Risk Management Program

An intelligence-led, expert-driven, strategic approach to global cybersecurity challenges affecting your organisation – your people, your operations, and your reputation.

On 17 February 2023, the Critical Infrastructure Risk Management Program (CIRMP) requirements came into effect. The clock is now ticking for more than 11,000 Australian critical infrastructure entities[1] to implement and become compliant with the risk management program obligations under the Security of Critical Infrastructure (SOCI) Act.

KEY SOCI MILESTONES

2 Apr 2022
Security of Critical Infrastructure Act Amendment came into effect

8 July 2022
Mandatory cybersecurity incident reporting obligation

8 Oct 2022
Critical infrastructure asset register reporting obligation

17 Aug 2023
Deadline to adopt a CIRMP

28 Sept 2023
Voluntary Board approved annual report to Commonwealth regulator

17 Aug 2024
Deadline to comply with the CIRMP requirements

28 Sept 2024
Deadline for Board approved annual report to Commonwealth regulator

The goal of the CIRMP is to help entities responsible for critical infrastructure assets establish, maintain and comply with a risk management program that takes a holistic and proactive approach to identifying and mitigating hazards that pose material risks to the availability, integrity, reliability or confidentiality of critical infrastructure assets.

The following sectors are subject to the CIRMP obligations:

- energy
- water and sewerage
- data storage
- financial services
- transportation
- food and grocery
- healthcare and medical
- communications

There are four key domains within the CIRMP that organisations 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;
- 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.

NEXT STEPS

Entities in scope will need to have a CIRMP in place that documents material risks and controls that will minimise material risks to your assets for each of the four key domains by 17 August 2023. Entities will have until 16 February 2024 to comply with the controls as defined in their CIRMP.

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.

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 their Critical Infrastructure Risk Management Program (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.

1 Critical Infrastructure Information Sharing and Analysis Centre (CI-ISAC), https://ci-isac.com.au/

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

TIM DE SOUSA
Senior Director
Information Governance, Privacy & Security
+61 2 9235 9305
tim.desousa@fticonsulting.com

03202023 | VN02678-v04