Security of Critical Infrastructure Act

Critical Infrastructure Risk Management Program

Australia's critical infrastructure landscape has been undergoing a major shift. Under the Security of Critical Infrastructure Act 2018 ("SOCI Act"), organisations across 11 key sectors have become subject to legally mandated security and reporting requirements. The Act requires owners and operators of essential assets to implement a formal, board-approved Critical Infrastructure Risk Management Program ("CIRMP"), and align with an appropriate cybersecurity framework. FTI Consulting can support your organisation in meeting SOCI Act obligations and strengthening overall resilience.

KEY OBLIGATIONS

Annually

— Organisations must submit an annual board-approved CIRMP to the Department of Home Affairs.

Ongoing

— Regular review and maintenance of the CIRMP (e.g., update when risk landscape changes, when new hazards emerge, or if the asset's characteristics change). If new critical infrastructure assets are acquired or identified, the organisation has six months from classification to implement a CIRMP and (later) meet the cybersecurity framework.

Immediately

— Significant cybersecurity incidents must be reported to the Australian Cyber Security Centre ("ACSC") within the timeframes defined by the SOCI Act (e.g. within 12 hours for critical incidents, or 72 hours for others).

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 11 sectors are subject to the CIRMP obligations:

— Communications

— Data storage or processing

— Defence industry

— Energy

— Financial services and markets

— Food and grocery

— Higher education and research

— Healthcare and medical

— Space technology

— Transport

— Water and sewerage

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.

How We Can Help

The experts at FTI Consulting will work with your organisation to define, implement and maintain a CIRMP and ensure compliance with the 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 identify gaps, realise security control improvements and improved all-hazards risk management practices.

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 significant 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.

CASE STUDY

Risk Management & Compliance for a Critical Infrastructure Energy Provider

OVERVIEW

FTI Cybersecurity was engaged to assist with preparing for, and complying with the Security of Critical Infrastructure (SOCI) Act. The scope comprised registration of multiple critical infrastructure (CI) assets, and development of a Critical Infrastructure Risk Management Program.

OUR ROLE

FTI Cybersecurity assisted the client with the registration of multiple CI assets, as the first step in meeting SOCI compliance obligations. This required gathering detailed information about the assets, their coverage and services, third-party suppliers and contractors, data storage arrangements, the holding company, and relevant supporting information. Determining which assets meet defined thresholds and considered in-scope was the first stage.

The next stage involved developing and documenting a Critical Infrastructure Risk Management Program (CIRMP) to ensure the company was compliant with new critical infrastructure legislation. The program includes risk assessment and treatment plans available or required in response to four key hazard vectors to be considered in a CIRMP: physical security and natural, cyber and information security, personnel, and supply chain.

Our team reviewed company documentation to better understand risk management approaches and existing security controls before conducting interviews with stakeholders. FTI Cybersecurity shared recommendations for next steps, supporting the approach and ongoing obligations to maintain compliance.

Additionally, we completed an assessment of the client's corporate network against cybersecurity requirements, using the Australian Energy Sector Cybersecurity Framework (AESCSF) to assist in improving security maturity, and to meet part of the SOCI Act's compliance obligations.

OUR IMPACT

With the help of FTI Cybersecurity, the client was able to unpick complexities and specific SOCI compliance requirements to help meet their regulatory obligations, significantly reducing their cybersecurity risk.

The client has subsequently engaged FTI Cybersecurity to support additional Risk Management Program activities and has recently undergone a Critical Infrastructure Security Centre (CISC) audit, which they passed with a clean bill of health.

1982

Year founded

34

Offices in 34 countries and teritories around the globe

800+

Senior Managing Director

8,370+

Employees worldwide

71

Advisor to 71 of the top 100 private equity firms as ranked by the Private Equity International 300 list

817

Ranked 817 on the fortune 1000

90

Advisor to 90 of the Fortune 100 corporations

100

Advisor to all 100 of the world's top 100 law firms as ranked by *The American Lawyer* Global 100 list

WOUTER VEUGELEN
Senior Managing Director & Head of Cybersecurity, Australia
+61 2 9235 9309
wouter.veugelen@fticonsulting.com

NATASHA PASSLEY
Senior Managing Director
+61 2 8247 8070
natasha.passley@fticonsulting.com

ED HOPKINS
Senior Director
+61 2 9235 9343
ed.hopkins@fticonsulting.com