Critical Infrastructure Risk Management Program

Part 2A *Security of Critical Infrastructure* (SOCI) *Act 2018* Factsheet

This guidance material has been prepared to assist in the understanding of the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006), subordinate legislation to the *Security of Critical Infrastructure Act 2018* (SOCI Act)

What is the CIRMP obligation?

The Critical Infrastructure Risk Management Program (CIRMP) is intended to uplift core security practices that relate to the management of certain critical infrastructure assets. It aims to ensure responsible entities take a holistic and proactive approach toward identifying, preventing and mitigating risks.

Responsible entities of the asset classes listed in the SOCI Act Application Rules are required to establish, maintain, and comply with a written risk management program that manages the 'material risk' of a 'hazard' occurring, which could have a relevant impact on their critical infrastructure asset.

Responsible entities must identify, and as far as is reasonably practicable, take steps to minimise or eliminate these 'material risks' that could have a 'relevant impact' on their asset.

The *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* (ERP Act) clarifies that the protection of certain business critical data and the secondary systems that store it should be considered under the CIRMP obligations. To enact obligations relating to risks to data storage systems holding 'business critical data' as 'material risks', the *Security of Critical Infrastructure Amendment (2025 Measures No. 1) Rules 2025*.

Additionally, Schedule 5 of the ERP Act uplifts, enhances and clarifies current security and related obligations under the Telecommunications Sector Security Reforms (TSSR) into the SOCI Act. The ERP Act is supported by the *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025* (TSRMP Rules). The TSRMP Rules commenced on 4 April 2025, and apply to those responsible entities that own and/or operate a carrier asset or relevant carriage service provider asset. Further guidance on the TSRMP Rules can be found on the CISC website.

Principles-based outcomes

The SOCI Act and *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (the Rules) specify requirements to be contained in a CIRMP. These requirements are based on the following principles-based outcomes:

- Identify material risks – Entities have a responsibility to take an all-hazards approach when identifying hazards that may affect the availability, integrity, reliability and confidentiality of their critical infrastructure asset.
- Minimise risks to prevent incidents – Entities are required to consider risks to their critical infrastructure asset (cyber and information security hazards, personnel hazards, supply chain hazards and physical security and natural hazards) and establish appropriate strategies to minimise or eliminate the risk of hazards occurring, so far as is reasonably practicable. Entities should consider both proactive risk management as well as establishing and managing processes to detect and respond to threats as they are being realised to prevent the risk from eventuating.
- Mitigate the impact of realised incidents – Entities are required to have robust procedures in place to mitigate, so far as is reasonably practicable, the impacts of a hazard, and recover from that impact as quickly as possible.
- Effective governance - Entities are required to provide an annual report that has been signed by their board, council or other governing body, to the relevant regulator and in some instances the Secretary of the Department of Home Affairs. The approved form that has been signed by a board, council or other governing body must be submitted along with the annual report. The annual report does not need to contain the CIRMP but must be sufficient to assure the relevant regulator that the program is up-to-date and appropriate.

What assets are affected by the obligations?

The Rules apply to the following critical infrastructure assets:

- critical electricity assets
- critical energy market operator assets
- critical gas assets
- critical liquid fuels assets
- critical water assets
- critical financial market infrastructure assets used in connection with the operation of payment systems
- critical data storage or processing assets, including secondary systems
- designated hospitals (listed in the Rules)
- critical domain name systems
- critical food and grocery assets
- critical telecommunications assets (via separate rules, Telecommunications guidance)

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter and LinkedIn

April 2025

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

- critical freight infrastructure assets (Rule 8 of the Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021 specifies that intermodal transfer facilities mentioned in schedule one of the instrument will be critical to the transportation of goods between states or territories. At this stage, only these facilities are subject to positive security obligations).
- critical freight services assets
- critical broadcasting assets

What is a material risk?

A risk is a material risk to a critical infrastructure asset when the risk has a relevant impact on the asset. Rule 5 (a-g) of the Rules provides the parameters of material risk. These include the risk of impairment, stoppage, loss of access to or interference with the asset.

What is a relevant impact?

A 'relevant impact' is an impact on the availability, integrity, and reliability of the asset, and the impact on the confidentiality of information about the asset, information stored in the asset if any, and, if the asset is computer data, the computer data.

The relevant impact may be direct or indirect. It must be more serious than a reduction in the quality of service being provided.

CIRMP Hazard Rules

The Rules contain obligations relating to protections within four key hazard vectors:

- Cyber and information security – 'cyber' risks to digital systems, computers, datasets, and networks that underpin critical infrastructure systems.
- Personnel – the 'trusted insider' risk posed by critical workers who have the access and ability to disrupt the functioning of the asset.
- Supply chain – risk of disruption to critical supply chains leading to a relevant impact on the critical infrastructure asset. The threat could be naturally occurring, malicious or purposefully intended to compromise the critical infrastructure asset.
- Physical and natural – physical risks to parts of the asset critical to the functioning of the asset, including physical access to sensitive facilities (e.g., control rooms) or natural disasters.

What does 'so far as it is reasonably practicable' mean?

The requirement to minimise or eliminate material risks 'so far as it is reasonably practicable' advises the responsible entities to act at a particular time that is reasonably possible to address those risks.

In considering the material risks to their business, responsible entities must weigh up what can be done to mitigate those risks - i.e., what is possible in the circumstances and whether those actions are reasonable in the circumstance. There is no expectation that entities pursue risk mitigation measures that are disproportionate relative to the likelihood and consequences of a particular risk.

The requirement provides responsible entities flexibility to determine how they address material risk and relevant impact in relation to their business size, maturity, income and overall asset criticality. The intent is for responsible entities to seek to minimise or eliminate material risk where it is reasonably possible, in order to secure their critical infrastructure asset.

In the annual attestation the Board, Council or other governing body (if the entity has one) are required to approve the risk management plan and in doing so, appropriately balance the costs of risk mitigation measures with the impact of those measures in reducing material risk within their own operational context.

What are the annual reporting requirements?

Entities are required to provide an annual report to the relevant Commonwealth regulator or the Secretary of the Department of Home Affairs, regarding the entities' CIRMP. Entities must submit this report within 90 days after the end of the financial year and the report must be approved by the entity's board, council, or other governing body.

The report must be in the approved form and state whether the risk management program was up to date, any variations to the program, and details of how the program was effective in mitigating any relevant impacts that hazards may have had on that asset during that year.

The report does not need to contain the full risk management program, but must be sufficient to assure the relevant Commonwealth regulator or the Secretary that the program remains up to date and appropriate.

The online annual reporting form can be found here: Responsible Entity Risk Management Program - Annual Report

The **2023-24 trial audits** indicated that common deficiencies in critical infrastructure risk management programs related to:

Personnel management – lack of insider threat mitigation and policies to identify critical workers

Physical hazard – lack of formal documented processes, guidelines and review mechanisms

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter and LinkedIn

Australian Government Department of Home Affairs | CYBER AND INFRASTRUCTURE SECURITY CENTRE

April 2025

Review and Remedy power

Reforms to the SOCI Act under section 2A allow the regulator last resort powers to direct an entity to remedy their risk management program, should it be found to be seriously deficient and not meeting the minimum protective standards. ‘Serious deficiency’ is defined as one that poses a material risk to the national security, defence, or social or economic stability of Australia or its people.

The power is managed with appropriate oversight mechanisms, with guidance and good-faith consultation remaining the first course of action to correct an identified deficiency in a risk management program. The regulator must first engage with the entity, alerting them to their intention to issue a direction and present them with an opportunity to respond before a direction can be issued.

The Department’s intention is that where deficiencies are identified, these directions would be issued in accordance with the Cyber and Infrastructure Security Centre’s (CISC) Compliance and Enforcement Strategy. The CISC seeks to work in partnership with industry to ensure regulated entities understand and effectively manage their risks, reserving compliance levers as last resort measures.

While risk management programs will not be required to be submitted to the CISC as a matter of course; entities will continue to be required to submit an annual attestation within 90 days of the end of the financial year – for further information refer to Guidance for the Critical Infrastructure Risk Management Program.

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter and LinkedIn

April 2025

Australian Government
Department of Home Affairs
CYBER AND INFRASTRUCTURE SECURITY CENTRE