Critical Infrastructure Risk Management Program
Managing personnel hazards

Part 2A of the Security of Critical Infrastructure Act 2018 (SOCI Act), and the associated critical infrastructure risk management program Rules 2023 and telecommunications security and risk management program (TSRMP) Rules 2025, require entities to manage personnel security risks under their risk management programs.

Your obligations under the SOCI Act:

As the responsible entity for a critical infrastructure asset, you may have obligations to ***implement, maintain, and comply*** with a critical infrastructure risk management program (CIRMP). Similarly, a bespoke CIRMP for responsible entities for critical telecommunications assets is applied through the TRSMP Rules.

The CIRMP is an opportunity to 'think big' and take an 'all hazards approach' in managing material risks to your business. Responsible entities must address four hazard vectors in their CIRMP:

- Cyber and information security;
- Personnel;
- Supply Chain; and
- Physical security and Natural.

Sector	Asset Class
Communications	Broadcasting
	Domain Name Systems Telecommunications*
Data Storage or Processing	Data Storage or Processing
Energy	Electricity
	Energy Market Operator
	Gas
	Liquid Fuels
Financial Services and Markets	Financial market Infrastructure (Payment Systems only)
Food and Grocery	Food and Grocery
Health Care and Medical	Hospitals
Transportation	Freight Infrastructure
	Freight Services
Water and Sewerage	Water

*applicable to carrier assets and carriage service provider assets that meet the threshold requirements. See Telecommunications guidance for more information

Mitigating personnel hazard risks:

An entity's CIRMP must establish and maintain a process or a system that:

a) Identify and list the entity's **critical workers**; and

b) Permits a **critical worker** access to **critical components** of the asset only where the worker has been assessed to be suitable to have such access; and

c) As far as it is reasonably practicable to do so, minimise or eliminate material risks arising from:

- Malicious or negligent employees or contractors
- The off-boarding process for outgoing employees and contractors

Standards and Frameworks – managing personnel hazards:

Entities may wish to consider the following standards and frameworks when developing their risk management program in relation to mitigating personnel hazards:

- AS 4811 – Employment Screening
- HB 323 – Employment Screening Handbook
- HB 167 (Security Risk Management)
- The Information Security Management Framework (ISMF) Part 10 – Workforce Management Security
- AS/NZS ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security controls – 'Human Resources Security'
- AS 8000 – Fraud and Corruption Control

Our compliance posture:

The CISC's approach to regulation is outlined in our Compliance and Enforcement Strategy.

The CISC recognises that businesses are best placed to determine ways to minimise or eliminate hazards that may have a relevant impact on their business. Furthermore, the CISC encourages business to identify all critical workers that have access to critical components to their assets. This includes having an effective on-boarding and off-boarding process for employees to ensure access is controlled which minimises personnel hazards.

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

April 2025

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

What is a critical worker?

A ***critical worker*** is an employee, intern, contractor, or subcontractor of an entity to which the CIRMP obligations applies; and

a) The entity assesses that their absence or compromise would prevent the proper function of the critical infrastructure or could cause significant damage to the asset; and

b) The individual has access to, or control and management of, a critical component of the asset

> Critical workers may have diverse working arrangements, including a permanent employee, contractor, or subcontractor status.
>
> All critical workers must be assessed at the same standard, *regardless of their length of employment*. For example, short-term contractors must be held to the same standard as permanent employees filling similar positions.

What is a critical component?

Part of the critical infrastructure asset that, if absent, damaged or compromised, the entity assesses:

a) Would prevent the proper function of the asset; or

b) Could cause significant damage to the asset;
as assessed by the responsible entity for the asset.

It is important to note that certain secondary systems that store or process business critical data, and satisfy section 9 (7) of the Act, form part of a critical infrastructure asset and are therefore considered critical components.

How to identify critical workers in your business:

a) Identify the 'critical component/s' of your asset

b) Identify the individuals that are essential to the proper functioning of the asset

c) Identify the workers with access, control, or management of the critical component/s of the asset.

> Critical workers could occupy roles such as Chief Information Security Officer or Control Room Operator or workers such as IT administrators with full and unrestricted administrator rights and access.

Reporting in your CIRMP:

- **Listing your critical workers:**

The responsible entity is required to list the individual and their held position in their CIRMP, and include justification for why that individual is a critical worker.

- **How long do I have to identify the critical workers?**

Entities must identify their critical workers and have commenced the process required to assess those critical workers on an ongoing basis by the end of the financial year.

How do I manage my critical personnel risks?

Managing personnel hazards should be approached holistically as part of the general obligation to manage material risks to an asset.

- **Background checks:**

Background checks are not mandatory, but may be a useful tool to assess the suitability of critical workers to undertake certain functions.

It is up to individual entities to decide how to best assess the risks critical workers could pose, and implement systems and/or processes to manage these risks.

- **Managing access to critical systems and assets**

It is important that only current critical workers have access to your critical systems. You should ensure that systems access, and physical access are revoked when staffing changes occur.

- **Regularly monitor activity to detect unauthorised actions**

Ensuring that there is continuous monitoring of access will allow you to detect and manage any breaches that occur. This will minimise the harm should an incident occur.

Insider threat case studies

There have been numerous instances of data exposure, theft or leak via insider threat in the last financial year. Insider threat refers to the risk posed by critical workers who have access to sensitive or confidential information, and the ability to disrupt the functioning of an asset.

Below are a de-identified examples of cyber incidents caused by insider actors:

Example 1: *A contracted employee of a critical infrastructure asset downloaded extensive amounts of confidential data to a personal hard drive upon their resignation at the company. This included technical plans/details on the layout of the facility and operational data.*

Example 2*: An employee at a critical infrastructure asset forwarded numerous emails to their personal email account, with attachments that contained sensitive confidential information about the asset. The employee then went overseas on holidays, and as such, the company were unable to verify the sensitive information had been contained.*

Example 3: *An employee didn't have their systems access revoked after leaving the organisation. They subsequently used their access to download sensitive information.*

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

Australian Government
Department of Home Affairs
CYBER AND INFRASTRUCTURE SECURITY CENTRE

April 2025