Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE

Critical Infrastructure Risk Management Program Guidance

Security of Critical Infrastructure Act 2018



© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (**www.creativecommons.org/licenses**).

This means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (**www.creativecommons.org/licenses/**).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (**www.pmc.gov.au/honours-and-symbols/commonwealth-coat-arms**).

Contact us

Enquiries regarding the licence and any use of this document are welcome to **CI.Guidance@homeaffairs.gov.au** or:

Critical Infrastructure Security Policy,
Department of Home Affairs
PO Box 25, BELCONNEN, ACT 2616

Notice - Nothing in this guidance necessarily binds the Department in the application of the SOCI Act or Rules. The Department may withdraw or replace the guidance at any time without further notice. The guidance represents the views of the Department only and a court may ultimately reach a different view on the interpretation of the provision

Table of contents

Table of contents 1
Acknowledgements 4

How to use this guidance 5
Chapters in this guidance 5

1. Introduction to the critical infrastructure risk management program (CIRMP) 7
1.1 What is a CIRMP? 7
1.2 Why is it important to have a CIRMP? 8
1.3 Asset classes with CIRMP obligations 9
1.4 Navigating multiple risk management program obligations 10
1.5 Timeframes for complying with CIRMP obligations 11
1.6 Requirements for a CIRMP 12

2. All hazards 15
2.1 Obligations for managing all hazards 15
2.2 Meeting the obligations in practice 17
2.2.1 Identify the operational context of the CI asset 17
2.2.2 Identify the material risks to the CI asset 19
2.2.3 Minimise or eliminate a material risk, and mitigate the relevant impact 21
2.2.4 Minimise or eliminate the material risks (enhanced) 25
2.3 Best practice for identifying and mitigating risks 28
2.4 Worked example – CIRMP entry 29

3. Cyber and information security hazards 32
3.1 Obligations for managing cyber and information security hazards 32
3.2 Meeting the obligations in practice 34
3.2.1 Minimise or eliminate a material risk, and mitigate the relevant impact 34
3.2.2 Comply with a cyber security framework 35
3.2.3 Minimise or eliminate specified material risks 42
3.2.4 Risk arising from failure to patch or update operating or security systems in a timely manner 42
3.3 Best practice for identifying and mitigating risks 45
3.4 Worked example – CIRMP Entry 52

4. Credential compromise hazards 55
4.1 Obligations for managing a credential compromise hazard 56
4.2 Meeting the obligations in practice 57
4.2.1 Outline the systems or networks where phishing resistant (MFA) is required to authenticate 57
4.2.2 Minimise or eliminate a material risk, and mitigate the relevant impact 57
4.2.3 Implement phishing resistant MFA 58
4.2.4 Centrally log, monitor, and review MFA attempts 59
4.3 Best practice for identifying and mitigating risks 59
4.4 Worked example – CIRMP entry 59

5. Lateral movement hazards 62
5.1 Obligations for managing lateral movement hazards 62
5.2 Meeting the obligations in practice 63
5.2.1 Identify and maintain an inventory of critical systems 63
5.2.2 Recovery, restoration and maintaining availability 63
5.2.3 Continued availability while rebuilding or restoring critical systems 64

5.2.4 Minimise or eliminate material risks and mitigate relevant impacts 64
5.2.5 Implement network segregation 65
5.3 Best practice for identifying and mitigating risks 66
5.4 Worked example – CIRMP entry 67
6. Personnel hazards 69
6.1 Obligations for managing personnel hazards 70
6.2 Meeting the obligations in practice 71
6.2.1 Identify the critical workers 71
6.2.2 Restrict access to critical workers assessed to be suitable 73
6.2.3 Minimise or eliminate specified material risks 75
6.2.4 Minimise or eliminate the material risks (enhanced) 76
6.2.5 Suitability assessment of critical workers that have access to critical components 78
6.2.6 Monitor suitability of critical workers 80
6.3 Best practice for identifying and mitigating risks 81
6.4 Worked example – CIRMP entry 88
7. Supply chain hazards 91
7.1 Obligations for managing supply chain hazards 92
7.2 Meeting the obligations in practice 93
7.2.1 Minimise or eliminate a material risk, and mitigate the relevant impact 93
7.2.2 Supply chain mapping for major suppliers and critical components 99
7.2.3 Vendor assessment for proposed or existing major suppliers 101
7.3 Best practice for identifying and mitigating risks 103
7.4 How to map supply chains 106
7.5 Illustrative case studies 120
7.6 Worked Example – CIRMP Entry 121
8. Physical security and natural hazards 124
8.1 Obligations for managing physical security and natural hazards 125
8.2 Meeting the obligations in practice 126
8.2.1 Identify physical critical components of the CI asset 126
8.2.2 Minimise or eliminate a material risk, and mitigate a relevant impact 127
8.2.3 Respond to incidents where unauthorised access to a physical critical component occurs 127
8.2.4 Control access to physical critical components 128
8.2.5 Test arrangements to detect, delay, deter, respond to, and recover from unauthorised access 129
8.2.6 Centrally manage physical security and natural hazards 130
8.2.7 Outline and consider risk associated with other hazards which impact physical security 131
8.3 Best practice for identifying and mitigating risks 132
8.4 Worked Example – CIRMP Entry 136
9. Maintaining the CIRMP and annual reporting requirements 139
9.1 Obligations for maintaining the CIRMP 140
9.2 Meeting the obligations in practice 141
9.2.1 Establish and maintain a process or system to review the CIRMP to ensure compliance with 30AE of the SOCI Act 141
9.2.6 Establish and maintain a process or system to keep the CIRMP current to ensure compliance with 30AF of the SOCI Act 143
9.2.7 A responsible entity must have regard to certain matters in deciding to whether to adopt or vary the CIRMP 143

9.3 Annual reporting requirements 145
Attachment A: Glossary of terms 150
Attachment B: Glossary of material risks 164
Attachment C – Checklists for CIRMP obligations 167
Attachment D – Obligations tables 185
Attachment E – CIRMP entry examples 194

Acknowledgements

This guidance has been developed through the valuable contributions of stakeholders across industry and government. We sincerely thank all those who shared their time, expertise, and insights throughout the consultation and development process.

Their collective knowledge and practical experience have helped shape a guidance document that supports the implementation of effective Critical Infrastructure Risk Management Programs (CIRMPs) and assists entities in meeting their obligations under Part 2A of the Security of Critical Infrastructure Act 2018 (SOCI Act).

We hope this guidance provides practical value not only to regulated entities, but also to the broader organisations, partners, and communities that contribute to and rely on resilient critical infrastructure.

We greatly appreciate the commitment and collaboration of all contributors in developing this resource.

In particular we would like to acknowledge the contributions from:

- Trusted Information Sharing Network (TISN) members
- The members of the Resilience Expert Advisory Group (REAG)
- The members of the Supply Chain Expert Advisory Group (SCEAG)
- Commonwealth Government Partners
- Jason Brown, Carl Gibson and Peter Wilkinson - Members of the Australian and New Zealand Standards Joint Technical Committee on Risk Management - OB007

Preface

This guidance has been prepared to assist responsible entities of critical infrastructure assets to adopt and maintain a critical infrastructure risk management program (CIRMP) in accordance with the *Security of Critical Infrastructure Act 2018* (SOCI Act) and the requirements set out in the *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules* (the CIRMP Rules).

The information contained in this document is general in nature and does not constitute legal advice.
If readers are unsure about their obligations to adopt and maintain a CIRMP in accordance with the SOCI Act and this guidance, they are encouraged to seek legal advice relevant to their particular circumstances.

How to use this guidance

The guidance includes the legal requirements as well as best practice approaches to compliance with the CIRMP obligations. This is to make it clear what entities are required to do and what is suggested as best practice.

Each chapter focuses on a specific aspect of CIRMP implementation. Many obligations, concepts and best practice approaches apply across multiple hazard types. As a result **there is a deliberate level of overlap between chapters**.

This document uses colour coding to indicate what framework is required to comply with obligations or consider material risks.

	This colour is used for guidance that is considered best practice
	This colour is used when entities subject to the enhanced CIRMP must comply with the information
	This colour is used when entities subject to the baseline CIRMP must comply with the information
	This colour is used when entites subject to the telecommunications security risk management program must comply with the information

Chapters in this guidance

Chapter 1. Introduction

Chapter 2. All hazards

Chapter 3. Cyber and information security hazards

Chapter 4. Credential compromise hazards

Chapter 5. Lateral movement hazards

Chapter 6. Personnel hazards

Chapter 7. Supply chain hazards

Chapter 8. Physical security hazards and natural hazards

Chapter 9. Maintaining the CIRMP and annual reporting requirements

Attachment A. Glossary of terms

Attachment B. Glossary of material risks

Attachment C. Checklist for CIRMP obligations

Attachment D: Obligations tables

Attachment E: CIRMP entry examples

Table of contents: Chapter 1

1.1 What is a CIRMP? 7
1.2 Why is it important to have a CIRMP? 8
1.3 Asset classes with CIRMP obligations 9
1.4 Navigating multiple risk management program obligations 9
1.4.1 Example of responsible entity with multiple assets 10
1.5 Timeframes for complying with CIRMP obligations 11
1.5.1 Baseline CIRMP 11
1.5.2 Enhanced CIRMP 11
1.5.3 Annual reporting 11
1.5.3.1 Enhanced CIRMP – Annual Reporting 11
1.6 Requirements for a CIRMP 12
1.6.1 Material Risk? 12
1.6.2 'So far as it is reasonably practicable' 13
1.6.2.1 Documenting decisions about what is 'so far as it is reasonably practicable' 13

1. Introduction to the critical infrastructure risk management program (CIRMP)

1.1 What is a CIRMP?

Part 2A of the *Security of Critical Infrastructure Act 2018* requires responsible entities to adopt and maintain a CIRMP. The *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023* (the CIRMP Rules) sets out requirements for a responsible entity's CIRMP.

A CIRMP is a written program that applies to a responsible entity and identifies and manages risks that could have an impact on a critical infrastructure asset (CI asset). A CIRMP must identify each hazard where there is a **material risk** that the **hazard** could have a **relevant impact** on the CI asset. The responsible entity must then, so far as it is reasonably practicable to do so, **minimise or eliminate the risk of the hazard occurring and mitigate the impact** if it occurs. The responsible entity must ensure the CIRMP is complied with, reviewed regularly, and updated where necessary – see Chapter 9 – **Maintaining the CIRMP and annual reporting requirements**.

Requirements for certain critical telecommunications assets are included in the *Security of Critical Infrastructure (Telecommunications Security Infrastructure and Risk Management Program) Rules 2025 LIN 25/010* (TSRMP Rules).

Guidance for Responsible Entities for Critical Telecommunications Assets outlines these requirements. Some content in this guide may assist responsible entities in implementing the obligations included in the TSRMP Rules.

A CIRMP is not required to be a single document. It can be a collection of policies, procedures, and supporting documents that together form a comprehensive program for managing risks. Responsible entities likely have established methods for identifying and managing risks. If the CIRMP consists of multiple documents, then the responsible entity should maintain a record of which documents are intended to satisfy each requirement in of the CIRMP Rules.

It is best practice for a CIRMP to include:

- A governance framework outlining those responsible for each component of the program, how decision-making in relation to the program will be done, and escalation processes.
- A process for risk identification and assessment that ensures responsible entities can identify threats and vulnerabilities and assess the level of associated risk.
- Strategies to mitigate, transfer, or accept identified risks.
- Plans for responding to and recovering from incidents.
- Processes for regular review and update, as well as lessons learned from incidents and exercises.
- Documentation to demonstrate compliance with regulatory requirements.

The CIRMP Rules outline specific hazard vectors for responsible entities to consider. Each hazard vector has a chapter of guidance within this package dedicated to it.

The CIRMP obligation encompasses layers of security, which are discussed throughout this guidance

CIRMP – Baseline	The baseline CIRMP is the lowest level of CIRMP obligation currently applied.
CIRMP – Enhanced	The enhanced CIRMP is applied to high-risk asset subclasses. The enhanced CIRMP has all the requirements of the baseline CIRMP as well as additional requirements. All entities are encouraged to comply with the enhanced CIRMP level.
TSRMP	The TSRMP is applied to certain critical telecommunications assets. The TSRMP has all the baseline requirements as well as additional specific requirements.

1.2 Why is it important to have a CIRMP?

The CIRMP obligations in Part 2A of the SOCI Act, introduced in 2022, responds to an increasingly complex and interconnected risk environment. The obligation helps responsible entities ensure the provision of vital goods and services. CI assets face a broad spectrum of risks. The CIRMP is designed to acknowledge the multi-factored challenges presented across this spectrum.

A robust CIRMP benefits Australia's national security and the responsible entity for the CI asset. A robust CIRMP recovery from incidents, assists to protect business' reputation and financial viability. It can build trust with customers, partners, regulators and shareholders by providing assurance that critical services are adopting a baseline level of risk management. This obligation provides a mechanism to assist Boards and governing bodies to analyse and assess security postures and appropriately allocate resourcing within the organisation.

Disruption to CI assets can have profound consequences for businesses, governments and communities. Harmful incidents targeting CI assets can compromise resource security, disrupt supply and service continuity, erode public confidence, and damage long term economic growth. The CIRMP obligation establishes a **baseline of security** across Australia's critical infrastructure to ensure responsible entities are prepared, resilient, and accountable.

The CIRMP obligation provides government assurance that CI assets are meeting a minimum security expectation. It ensures that responsible entities are adopting a holistic and proactive approach in identifying, preventing, and mitigating material risks from all hazards. It also acknowledges the interconnected nature of hazard domains. Security practices in one hazard vector can have impacts across a range of other hazard vectors. The CIRMP obligation seeks to ensure responsible entity's risk management practices are not siloed and consider the cascading impacts across the whole organisation. This strengthens collective national security. The compromise of one vulnerable component of the Australian critical infrastructure network can have cascading impacts to the entire network.

The CIRMP was designed to complement existing risk management practices within the responsible entity's organisation. Responsible entities are encouraged to go beyond the requirements under the CIRMP Rules.

Compliance with the CIRMP obligation is the bare minimum of risk management

1.3 Asset classes with CIRMP obligations

Sector	Asset class	Baseline[1]	Enhanced	TSRMP
Energy	Critical electricity assets	✓	✓	
	Critical gas assets	✓	✓	
	Critical energy market operator assets	✓	✓	
	Critical liquid fuel assets	✓	✓	
Communications	Critical telecommunications assets			✓[2]
	Critical broadcasting assets	✓	✓	
	Critical domain name system assets	✓	✓	
Data Storage & Processing	Critical data storage or processing assets	✓		
Financial Services & Markets	Critical banking assets			
	Critical superannuation assets			
	Critical insurance assets			
	Critical financial market infrastructure assets	✓[3]		
Water & Sewerage	Critical water assets	✓	✓	
Healthcare & Medical	Designated hospital	✓[4]		
	Critical hospital assets			
Higher Education & Research	Critical education assets			
Food & Grocery	Critical food and grocery assets	✓		
Transport	Critical ports			
	Critical freight infrastructure assets	✓	✓	
	Critical freight services assets	✓	✓	
	Critical public transport assets			
	Critical aviation assets			
Space Technology	No assets currently defined			
Defence Industry	Critical defence assets			

1 As per Part 2AA, entities that are exempted under section 30AB(3)-(6) are not obligated to have a CIRMP, but may be obligated to provide an annual report.

2 Under the SOCI Act and TSRMP Rules – relevant critical infrastructure assets are obligated to comply with Part 2A of the SOCI Act. A relevant critical infrastructure asset is a critical telecommunications asset that is owned or operated by a carrier or a relevant carriage service provider asset (as defined in section 4 of the TSRMP Rules).

3 Only applies to an asset that is used in connection with the operation of a payment system that is critical to the security and reliability of the finance services and market sector, see section 12D(1)(i) of the SOCI Act.

4 For a complete list of designated hospitals see the CIRMP Rules at Schedule 1.

1.4 Navigating multiple risk management program obligations

Some responsible entities own or operate CI assets across multiple sectors and asset classes. As a result, a responsible entity may be subject to different risk management program obligations for different assets. Where an asset is subject to the enhanced CIRMP and/or TSRMP obligations, the responsible entity must implement the additional requirements. The responsible entity may choose to apply the additional requirements to all their assets for efficiency or consistency. All responsible entities are encouraged to implement controls beyond the baseline.

1.4.1 Example of responsible entity with multiple assets

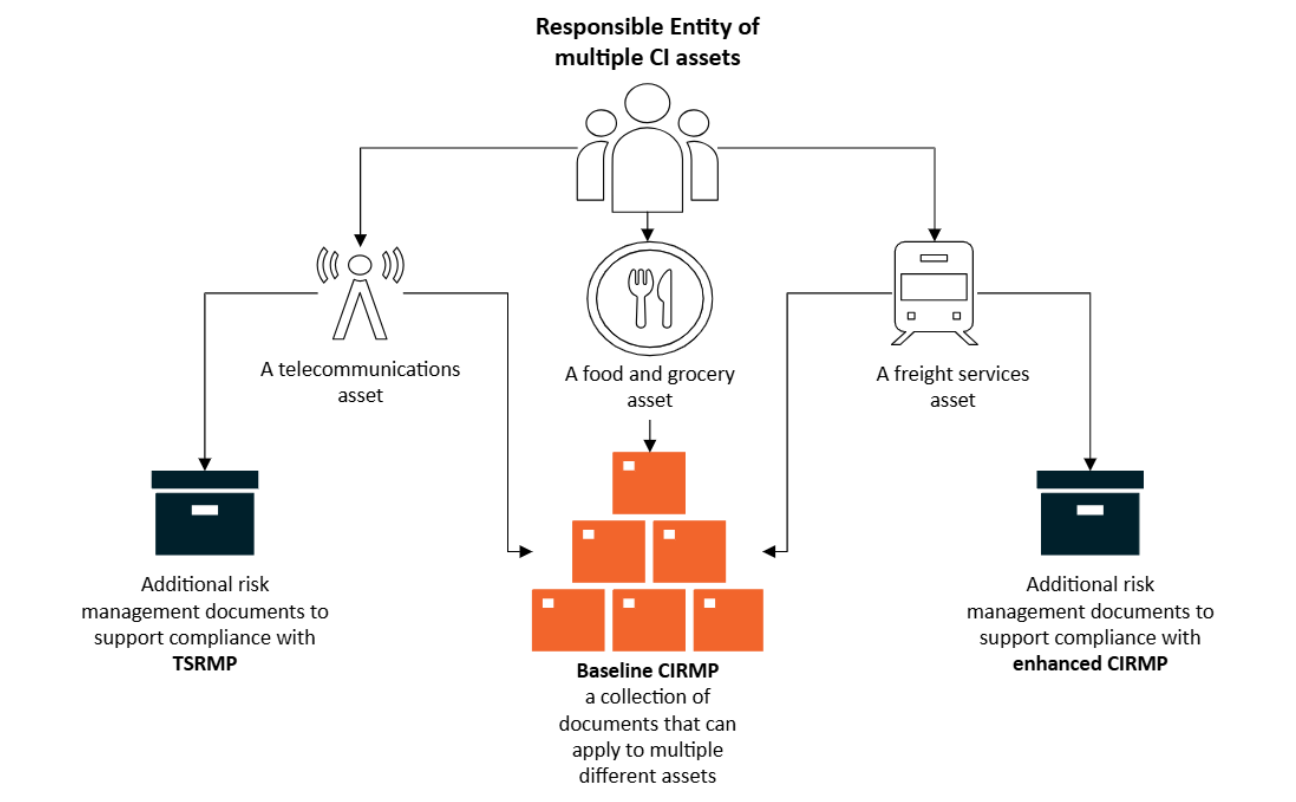
A responsible entity has a food and grocery asset, a telecommunications asset (that is a relevant CI asset under the TSRMP Rules), and a freight services asset.

- Each asset must comply with the baseline CIRMP.
- The telecommunications asset must comply with the TSRMP.
- The freight services asset must comply with the enhanced CIRMP.

The responsible entity is compliant with Maturity Level 1 of a cyber security framework prescribed in the baseline CIRMP. This framework is shared across all their assets.

The freight services asset must comply the enhanced CIRMP and must reach Maturity Level 2 of the cyber security framework. The responsible entity may elect to uplift all three assets.

Similarly, the telecommunications asset must comply with the TSRMP and must also reach Maturity Level 2. They may elect to voluntarily uplift the food and grocery asset.



1.5 Timeframes for complying with CIRMP obligations

1.5.1 Baseline CIRMP

When an asset becomes a CI asset, the CIRMP Rules provide a grace period for the responsible entity to comply with the CIRMP obligation. The grace period is 6 months after the asset becomes a CI asset or as otherwise provided in the CIRMP Rules.

1.5.2 Enhanced CIRMP

The enhanced CIRMP introduce new specified material risks, two new hazard vectors, and new measures across all of the existing hazard vectors. The new material risks and measures have staggered grace periods to acknowledge the time and cost of implementing the measures. The below timeframes apply to CI assets that were CI assets subject to the enhanced CIRMP before commencement of the instrument. In practice this means that if the CI asset was a CI asset subject to the enhanced CIRMP prior to 10 June 2026, these grace periods apply. The below dates refer to the last day of the grace period.

New material risks	Sections 6A, 8A(2) and 9A(2) of the CIRMP Rules	10 June 2027
All other measures	Sections 8A (other than subsection 8A(2)), 8B, 8C, 9A (other than subsection 9A(2)), 10A and 11A	10 June 2028

1.5.3 Annual reporting

Responsible entities must provide an annual report if they were the responsible entity for one or more CI assets during a period that consists of the whole or part of a financial year and were subject to the CIRMP obligation (section 30AG of the SOCI Act). The annual report must be provided to the relevant Commonwealth regulator within 90 days after the end of the financial year. For more information see Chapter 9 – **Maintaining the CIRMP and annual reporting requirements**.

1.5.3.1 Enhanced CIRMP – Annual Reporting

For entities subject to the enhanced CIRMP, the entities will need to provide their annual report in accordance with the above information (at 1.5.3), and in addition will have reporting requirements on the new material risks and other measures under the enhanced CIRMP.

In the 2026-27 annual report – responsible entities will need to report on the enhanced material risks, **beginning on 11 June 2027** until the end of the 2026-27 financial year.

In the 2027-28 annual report – responsible entities will need to report on the enhanced material risks for the entire financial year. For the other enhanced measures, responsible entities will need to report, **beginning on 11 June 2028** until the end of the 2027-28 financial year.

In the 2028-29 annual report – responsible entities will need to report on all enhanced CIRMP obligations for the entire financial year.

1.6 Requirements for a CIRMP

The SOCI Act requires responsible entities to adopt and maintain a CIRMP (section 30AC).

Under section 30AH of the SOCI Act, a CIRMP must, for each CI asset:

- Identify each hazard where there is a material risk (see 1.6.1) that the occurrence of the hazard could have a relevant impact on the asset.
- So far as it is reasonably practicable (see 1.6.2) to do so, minimise or eliminate any material risk of such a hazard occurring.
- So far as it is reasonably practicable to do so mitigate the relevant impact of such a hazard on the asset.

Part 2A of the SOCI Act is an all hazards framework. The CIRMP Rules provide **material risks** that should be considered and mitigated against for all CI assets. Responsible entities are best placed to understand the specific threats and vulnerabilities impacting their CI assets that go beyond the specified material risks.

For definitions of **hazard** and **relevant impact** see the **glossary**.

1.6.1 Material Risk?

'**Material risk**' is not specifically defined in the SOCI Act or the CIRMP Rules. 'Material' and 'risk' are given their ordinary meaning according to the Macquarie Dictionary.

A material risk might be a risk that extends beyond routine operational issues and could disrupt essential services, compromise national security, or cause significant consequences for a CI asset. Material risks may stem from a routine issue that evolves or has the potential to disrupt or compromise the CI asset and have cascading effects across other sectors.

As set out in s 30AH(7) of the SOCI Act, in determining whether a risk is a material risk, regard must be had to the likelihood of the hazard occurring and the relevant impact of the hazard on the asset if the hazard were to occur.

Sections 6 and 6A of the CIRMP Rules and s 8 of the TSRMP specify particular risks that must be taken to be material risks for the purposes of an entity's CIRMP. Those are set out in **Attachment B**.

In considering whether a risk is material, responsible entities should consider:

- **Severity of impact** – the potential consequences on the CI asset's ability to deliver its critical function, including impacts it may have on public safety, economic stability, or national security.
    - **Interdependencies** – the extent to which the risk could extend through other critical infrastructure sectors, thus amplifying the severity. If a risk has significant interdependencies, then it is more likely to be a material risk.
- **Operational and strategic consequences** – whether the risk could lead to prolonged service outages, significant financial loss, or regulatory non-compliance.
- **Likelihood of the hazard** – whether the occurrence of the hazard is probable.

For example, an asset that is located hundreds of kilometres inland would not generally be expected to mitigate the direct physical impacts of a tsunami on the asset. However, a responsible entity should consider indirect impacts (such as disruption to supply chains) and whether it constitutes a relevant impact on the asset.

When a material risk is identified, the responsible entity must, so far as it is reasonably practicable, minimise or eliminate that material risk.

1.6.2 ‘So far as it is reasonably practicable’

Section 30AH of the SOCI Act applies the legal doctrine of ‘so far as it is reasonably practicable to do so’ to the obligations to minimise or eliminate material risks and to mitigate relevant impacts on the CI asset.

Accordingly, a responsible entity must, so far as it is reasonably practicable to do so minimise or eliminate any material risk of such a hazard occurring; and mitigate the relevant impact of such a hazard on the asset.

In considering what is reasonably practicable in the circumstances, responsible entities should consider the following:

- The likelihood of the hazard or the risk occurring;
- The impact of the potential hazard or risk on the CI asset’s ability to function;
- The availability and suitability of ways to eliminate or minimise the risk; and
- The cost of eliminating or minimising the risk (including time, money, impact on productivity, or other resources.

Responsible entities cannot decline to implement a mitigation or control solely on the basis that it is inconvenient, or expensive. The responsible entity should be able to demonstrate that the cost is clearly excessive in relation to the risk.

“So far is it is reasonably practicable to do so’ requires informed, proactive, and documented consideration. A responsible entity should be able to demonstrate that all reasonable steps to protect the asset were taken unless further measures would be clearly excessive in relation to the risk.

1.6.2.1 Documenting decisions about what is ‘so far as it is reasonably practicable’

When making an assessment of what is ‘so far as it is reasonably practicable’ to implement, responsible entities should apply the standard in an objective manner. The documentation outlined below is provided as guidance and reflects best practice to support consideration of what is reasonably practicable and demonstrate how the standard should be applied. Documented decisions should set out four key parts:

Identify the hazard or risk

Provide a description of the hazard or risk, including the potential consequence if it were to occur and an assessment of the likelihood of an occurrence. Where the responsible entity is responsible for multiple assets, the documentation should clearly identify the relevant asset(s) and the basis on which they may be affected.

Outline the potential controls or mitigations

Identify and consider a range of reasonably available controls or mitigations. This supports an assessment that the responsible entity has considered practicable options. The documentation should outline how each control goes to eliminating or otherwise mitigating the risk and reduces the potential impact.

Assess ‘reasonably practicable’

Record the analysis that was conducted to determine whether the controls are reasonably practicable in the circumstances. This may include consideration of severity of impact; likelihood; effectiveness; and the cost or burden of implementation and why particular measures were not adopted.

Record the decision

Record the decision, including which controls will be implemented, any implementation timeframes, and the reasons for not adopting other measures. The documentation should also note review triggers (for example, changes in the threat environment or asset criticality).

Responsible entities are best placed to determine where this documentation should be maintained (for example, within the CIRMP or in supporting records). As guidance, it is recommended that the documentation is readily available to support internal governance and, where relevant, compliance and assurance activities.



Table of contents: Chapter 2

2.1 Obligations for managing all hazards 15
2.2 Meeting the obligations in practice 17
2.2.1 Identify the operational context of the CI asset 17
2.2.2 Identify the material risks to the CI asset 19
2.2.3 Minimise or eliminate a material risk, and mitigate the relevant impact 21
2.2.3.1 Risk arising from a stoppage or major slowdown of the CI asset's function for an unmanageable period 21
2.2.3.2 Risk arising from a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the CI asset 22
2.2.3.3 Risk arising from an interference with the CI asset's operational technology or information communication technology essential to the functioning of the asset 23
2.2.3.4 Risk arising from the storage, transmission or processing of sensitive operational information outside Australia 23
2.2.3.5 Risk arising from remote access to operational control or operational monitoring systems of the CI asset 24
2.2.3.6 Risk arising from impacts to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data 24
2.2.4 Minimise or eliminate the material risks (enhanced) 25
2.2.4.1 Impairment of the CI asset's functions that could prejudice the social stability, economic stability, national security or defence of Australia 25
2.2.4.2 Compromise or impairment of the functions of the CI asset as a result of, or in connection with FOCI 26
2.2.4.3 Risk arising from offshore or remote access to critical components 26
2.2.4.4 Risk arising from offshore or remote access to critical components 27
2.3 Best practice for identifying and mitigating risks 28
2.3.1 Material risks for consideration 28
2.3.2 Treating risk – mitigations and controls 28
2.4 Worked example – CIRMP entry 36

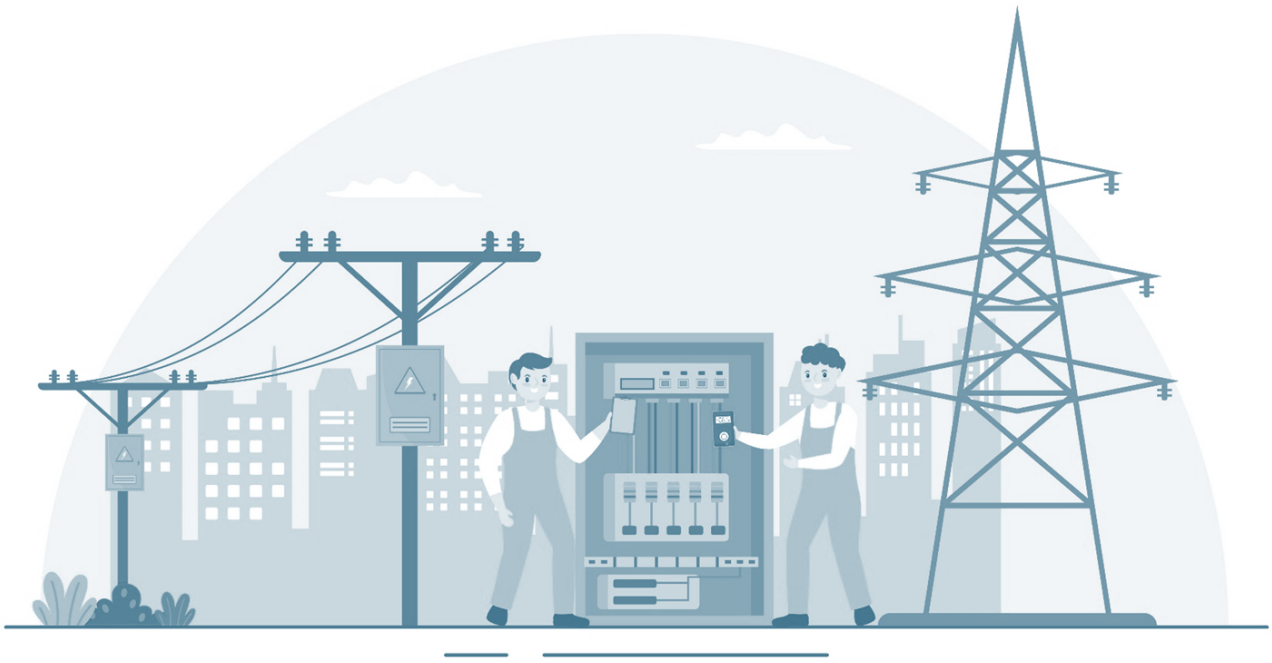
2. All hazards

The SOCI Act and CIRMP Rules require responsible entities to adopt an all hazards approach to risk management. This means responsible entities must consider and manage risks arising across all hazard vectors, as well as risks arising from hazards that do not fall within one of the specified hazard vectors. It also acknowledges that these hazard vectors do not operate in isolation, and there is a significant level of interconnectivity between the vectors. In practice, a single incident may involve multiple hazard vectors and lead to cascading impacts across the CI asset.

The all hazards approach seeks to ensure responsible entities take a holistic approach to managing risks and their impacts.

2.1 Obligations for managing all hazards

The table on the following page outlines the obligations in the CIRMP Rules in relation to all hazards. It outlines whether the obligations apply to entities subject to the baseline and/or enhanced CIRMP requirements and/or TSRMP requirements. The obligations are expanded on later in this chapter.



All hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Establish and maintain a process or system to identify the operational context of the CI asset.	s 7(1)(a)	s 7(1)(a)	s 9(a)
Establish and maintain a process or system to identify the material risks to the CI asset.	s 7(1)(b)	s 7(1)(b)	s 9(b)
Establish and maintain a process or system to – as far as it is reasonably practicable to do so – minimise or eliminate the material risks and mitigate the relevant impact of each hazard on the CI asset. The material risks may include: (a) A stoppage or major slowdown of the CI asset's function for an unmanageable period (b) A substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the CI asset Example - The position, navigation and timing systems affecting provision of service or functioning of the asset. (c) An interference with the CI asset's operational technology or information communication technology essential to the functioning of the asset Example - A Supervisory Control and Data Acquisition (SCADA) system. (d) The storage, transmission or processing of sensitive operational information outside Australia, which includes: (i) Layout diagrams (ii) Schematics (iii) Geospatial information (iv) Configuration information (v) Operational constraints or tolerances information (vi) Data that a reasonable person would consider to be confidential or sensitive about the asset (e) Remote access to operational control or operational monitoring systems of the CI asset (f) Impact to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data.	s 6 s 7(1)(c)	s 6 s 7(1)(c)	s 8 s 9(c)
Establish and maintain a process or system to – as far as it is reasonably practicable to do so – minimise or eliminate the additional material risks specified in subsection 6A(2) of the CIRMP Rules. The following specified risks are additional material risks: (a) any impairment of the CI asset's functions that could prejudice the social stability, economic stability, national security or defence of Australia; (b) compromise or impairment of the functions of the CI asset as a result of, or in connection with FOCI; (c) offshore or remote access to critical components; and (d) offshore or remote access to business critical data.		s 6A(1) s 6A(2)	

Timeframes for compliance are explained in Chapter 1 – **Introduction to the critical infrastructure risk management program (CIRMP)** at **1.5**

2.2 Meeting the obligations in practice

2.2.1 Identify the operational context of the CI asset

CIRMP baseline – sections 7(1)(a) of the CIRMP Rules

CIRMP enhanced – section 7(1)(a) of the CIRMP Rules

TSRMP – section 9(a) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must establish and maintain a process or system in the CIRMP to identify the operational context of the CI asset.

Understanding the operational context assists responsible entities to identify how the asset functions, what it depends on, and what hazards, vulnerabilities and interdependencies may influence its operation. This understanding forms the foundation for identifying material risks and implementing appropriate mitigations within the CIRMP.

Operational context is explained in the **glossary**

Step 1. Identify the function and core requirements of the CI asset

Responsible entities should first identify the proper function of the CI asset and the systems, people, processes and services required to support that function.

This may include consideration of:

- **Critical components** and **critical systems**.
- Key operational technology (OT) and information technology (IT) systems.
- Essential operational processes and procedures.
- Critical workers and workforce capability requirements.
- Major suppliers.
- Physical critical components and locations.
- Governance, management and decision-making structures

This step allows the responsible entity to understand the asset's core operational requirements and identify the elements that are essential to maintaining the delivery of the asset's critical function.

Step 2. Assess the internal environment

Understanding the internal environment assists responsible entities to identify operational vulnerabilities, single points of failure, and the ways internal systems and processes may contribute to or mitigate risk. It is recommended that responsible entities consider how their organisational structure, workforce, technology requirements, and governance will inform how they operate and manage risk and threat.

For example, a responsible entity with a highly specialised workforce and a dependency on specific vendors but limited physical critical components is likely to place more resources to mitigating their supply chain and personnel risks. This may inform how they operate and prioritise resources to manage risks. However, it's important to note that all risks, even those that are less significant, must still be considered. Having an understanding of the internal environment can ensure resources are appropriately managed and allocated.

Step 3. Assess the external environment

Responsible entities should consider identifying external factors that may influence the operation, resilience or security of the CI asset. This may involve assessing how external conditions may create hazards or operational constraints. CI asset locations can impact the operation of an asset in many ways across all hazard vectors. For example, there may be jurisdictional risk where CI asset components or workforces are geographically dispersed, or the location of an asset may put it at particular risk of natural hazard events.

Responsible entities may also consider their interdependencies at this step. The CI asset may be dependent on, or influenced by, other CI assets or sectors. If the responsible entity is highly dependent on a particular sector, and that sector faces specific issues, then it is recommended that the responsible entity consider how that may impact their CI asset.

Other infrastructure (critical or not) may impact the operation of the CI asset, such as building proposals that could impact the operation of the CI asset. In this circumstance the responsible entity is encouraged to consider this as part of their operational context and discuss with relevant bodies how they can influence the development of these proposals.

For example, the responsible entity is highly dependent on a data storage or processing provider, but they are not directly dependent on the water sector. The responsible entity is encouraged to consider how the data storage or processing provider may be impacted by disruption to their water supply and how this could cascade down to the responsible entity's CI asset.

This step ensures the responsible entity understands the broader environment in which the asset operates and the external dependencies that may influence risk exposure.

Step 4. Document and record the process

It is recommended that responsible entities ensure this process is clearly documented and repeatable. It is recommended that the responsible entity regularly review their operational context to ensure it is up to date based on changes to the environment. Ensuring this process is clearly documented will ensure this is more easily completed in the future.



2.2.2 Identify the material risks to the CI asset

CIRMP baseline – section 7(1)(b) of the CIRMP Rules

CIRMP enhanced – section 7(1)(b) of the CIRMP Rules

TSRMP – section 9(b) of the TSRMP Rules

A CIRMP must set out a process or system for identifying material risks to a CI asset. **Material risk** is explained in the **glossary**.

Identifying material risks allows for compliance with other obligations, as detailed in in **2.2**.

In implementing this, it is recommended that responsible entities establish a structured and repeatable process to identify all material risks, including those that are not already specified in the CIRMP Rules. This process should be embedded in the CIRMP and it is recommended that responsible entities consider the operational context of the CI asset when identifying material risks.

Step 1. Identify risks

It is recommended that responsible entities generate a comprehensive list of all risk scenarios that may impact the CI asset.

In generating this list, responsible entities should consider all hazard vectors (independent of likelihood or the level of impact it may have), the operational context of the asset (asset specific vulnerabilities), and how hazards may interact to create new, interdependent risks.

Step 2. Assess the potential impact of these risks

The purpose of a CIRMP is to identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the CI asset (s 30AH(1) of the SOCI Act). Therefore, responsible entities should understand the severity of consequences associated with each material risk.

Consider potential consequences should the risks eventuate to determine whether there could be a relevant impact on the CI asset. For more information on **relevant impact**, see the **glossary**.

When assessing the impact, consideration may be given to the scale and duration of the disruption, whether the impact would have cascading effects across other systems or components, and whether it would exceed defined tolerances for outages or reduced output.

Step 3. Assess the likelihood of these risks

Responsible entities are encouraged to undertake an evidence-based assessment of the likelihood of the risk eventuating. Responsible entities are encouraged to appropriately record the assessment so their CIRMP can be updated should circumstances change. In assessing the likelihood, the responsible entity can consider:

- the current threat environment
- historical incidents and near misses
- known vulnerabilities
- environmental conditions.

This is not an exhaustive list. Many factors will go to the likelihood of an incident occurring and it is the responsible entity's responsibility to undertake this assessment.

Step 4. Analyse whether this meets the definition of a material risk

Once the responsible entity has determined that:

- the material risk could result in a relevant impact on their CI asset, and
- that it is not improbable that the hazard would eventuate

then they must establish and maintain a process or system in the responsible entity's CIRMP to identify that material risk.

Responsible entities are encouraged to document in their CIRMP the assessment of whether a risk meets the threshold of a material risk. The process of identifying material risks should be undertaken regularly. It is recommended that documentation should form part of a responsible entity's review of their CIRMP and the CIRMP should be reviewed when circumstances for the CI asset change.

Example of material risk assessment

An example of this process is provided below:

Step 1. Identify risks	A critical water asset relies on a third-party cloud service provider to store operational data and process information. This interdependency presents a risk as the water asset is reliant on the provider to maintain its proper function.
Step 2. Assess the impact of risks.	If the provider is unavailable the responsible entity may lose access to real-time water quality data and operators may need to switch to manual processes, which reduce situational awareness. There would be a direct impact to the availability of operational monitoring systems and reduction in reliability of the water treatment process. This risk could result in a relevant impact on the critical water asset.
Step 3. Assess the likelihood of risks	In considering this risk the responsible entity assesses that cyber attacks against cloud service providers are increasing and there are known vulnerabilities in this type of provider. Conversely, the provider has a backup system and disaster recovery arrangements. The likelihood is possible given provided information.
Step 4. Analyse whether this meets the definition of a material risk.	The water treatment plant is dependent on the third-party cloud data storage and processing provider for operational monitoring, analytics, and regulatory reporting functions. A cyber incident, system failure, or prolonged outage affecting the provider may result in loss of operational visibility, reduced treatment capability, and delayed incident response. Given the credible threat environment and potential impacts on availability and reliability, this risk has been assessed as a material risk.

Throughout each chapter of this guidance there are suggested material risks. These risks should be considered, in addition to the material risks identified by the responsible entity.

2.2.3 Minimise or eliminate a material risk, and mitigate the relevant impact

CIRMP baseline – sections 6 and 7(1)(c) of the CIRMP Rules

CIRMP enhanced – sections 6 and 7(1)(c) of the CIRMP Rules

TSRMP – sections 8 and 9(c) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must establish and maintain a process or system in the entity's CIRMP to – as far as it is reasonably practicable to do so - minimise or eliminate the material risks and mitigate the relevant impact of each hazard on the CI asset.

Responsible entities should undertake this process for the material risks they identified as per **2.2.2**, as well as the material risks that are outlined below.

It is best practice for all entities to consider the material risks listed in the enhanced CIRMP, see **2.2.4** of this chapter. Best practice material risks are raised in all chapters of the guidance.

2.2.3.1 Risk arising from a stoppage or major slowdown of the CI asset's function for an unmanageable period

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must seek to minimise or eliminate the material risk of a stoppage or major slowdown of the CI asset's function for an unmanageable period (sections 6(a) and 7(1)(c) of the CIRMP Rules and section 8(a) of the TSRMP Rules).

To appropriately consider this risk, responsible entities will need to understand the proper function of the CI asset, and at what point a stoppage or slowdown would result in disruption to that function for an unmanageable period. In practice, this may involve scenarios such as a prolonged service outage, damage to key infrastructure, or the failure of systems that support the asset's core functions.

Step 1. Identify the point at which a disruption is unmanageable

An **unmanageable period** is the period of time where a stoppage or major slowdown prevents the function of the CI asset, which cannot be managed by reasonable contingencies or response and recovery measures. This period will be unique to each CI asset.

This period may be longer for responsible entities that have significant backup systems and redundancy capabilities. The term allows the responsible entity the flexibility to determine what period is unmanageable in their operating context.

Responsible entities should seek to determine how long their CI asset can function in the event that various components are made unavailable. Responsible entities may do this through tabletop exercising or previous lessons learned. Once this period is determined, responsible entities are encouraged to document this as part of the response and recovery processes for the CI asset.

Step 2. Identify potential causes for a stoppage or major slowdown

A stoppage may refer to the complete loss or halting of a CI asset's ability to deliver its functions.

A major slowdown may refer to a significant degradation of the CI asset's ability to deliver its functions.

Responsible entities should seek to identify potential causes for a stoppage or major slowdown so they can appropriately seek to eliminate and mitigate this material risk. The causes of stoppages or slowdowns may be varied and can include equipment failure, cyber incidents, workforce disruptions, supply chain issues, environmental events, or coordination failures between systems. In some cases, multiple contributing factors may interact to create or prolong the disruption. Responsible entities should therefore consider both single-point failures and compound events when identifying and assessing this risk.

In developing their CIRMP, responsible entities should ensure they have processes in place to identify the conditions under which a stoppage or major slowdown could occur, and to assess the potential duration and impact of such disruptions. This includes understanding system dependencies, capacity limits, and recovery timeframes.

Step 3. Identify and implement controls

Once potential causes are identified, responsible entities should consider how to minimise or eliminate the potential of these risks occurring, and seek to mitigate the impact they may have on the CI asset.

Responsible entities should consider measures to minimise the likelihood of disruption, and to maintain or restore service as quickly as possible if a disruption occurs. These measures may include redundancy arrangements, surge capacity, incident response procedures, and recovery planning to reduce the severity and duration of any stoppage or slowdown.

Example of a risk arising from a stoppage of the CI asset's functions

Step 1. Identify the point in which a disruption is unmanageable	A critical freight infrastructure asset, specifically a freight rail terminal, relies on a terminal management system to coordinate train arrivals and departures, container movements, and loading/unloading operations. Through an assessment of business continuity plans, operational exercising, and lessons learned from previous incidents, the responsible entity determines that manual work arounds for the terminal management system can only be managed for up to 12 hours. A disruption beyond 12 hours results in safety risks, congestion, and failure to maintain freight processing and terminal movements. For this CI asset, a stoppage of the terminal management system exceeding 12 hours is an unmanageable period.
Step 2. Identify potential causes for a stoppage or major slowdown	Through an assessment of the dependencies for the terminal management system, the responsible entity determines that cyber incidents, failure to patch or maintain software, and trusted insider threats could result in an impact on the terminal management system, which would subsequently result in a stoppage or major slowdown.
Step 3. Identify and implement controls	The responsible entity implements preventative controls such as scheduled maintenance, testing, software updates. They also implement processes to extend the period in which the stoppage can be managed. They do this by increasing their ability to manually work around the terminal management system and implementing a physical failover.

2.2.3.2 Risk arising from a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the CI asset

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must seek to minimise or eliminate the material risk arising from a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the CI asset (sections 6(b) and 7(c) of the CIRMP Rules and section 8(c) of the TSRMP Rules).

To assist responsible entities in considering this material risk, it is recommended they maintain a comprehensive record of their critical components. For physical security hazards and natural hazards, responsible entities are required to identify physical critical components (see **8.2.1** of Chapter 8 – **Physical security and natural hazards**) and responsible entities subject to the enhanced CIRMP are required to identify critical systems for lateral movement hazards (see **5.2.1** of Chapter 5 – **Lateral movement hazards**).

This material risk requires the responsible entity to consider how loss of access to, or manipulation of a critical component may impact the CI asset broadly. Critical components are vital for the function of the CI asset, as such a loss of access to or manipulation of these components can have severe consequences for the delivery of essential services.

Responsible entities should consider both direct and indirect impacts of loss of access or manipulation.

- Direct impacts may include system outages, loss of control, or degradation of service delivery.
- Indirect impacts may include reduced situational awareness, delayed response to incidents, or increased risk of cascading failures across interconnected systems.

Given the dependencies between components, failure or manipulation of one critical component may also trigger broader impacts across the CI asset.

In developing their CIRMP, responsible entities should ensure they have processes in place to identify vulnerabilities that could lead to loss of access or manipulation, and to detect and respond to such events. This may include measures such as layered access controls (**8.3.2.3** of Chapter 8 – **Physical security and natural hazards**), multi-factor authentication (**4.2.3** of Chapter 4 – **Credential compromise hazards**), and suitability assessments of personnel (**6.2.5** of Chapter 6 – **Personnel hazards**).

2.2.3.3 Risk arising from an interference with the CI asset's operational technology or information communication technology essential to the functioning of the asset

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must seek to minimise or eliminate the material risk arising from an interference with the CI asset's operational technology (OT) or information communication technology (ICT) essential to the functioning of the asset (sections 6(c) and 7(1)(c) of the CIRMP Rules and section 8(d) of the TSRMP Rules).

OT and ICT systems are fundamental to the control, monitoring and management of modern infrastructure, and interference with these systems can directly affect the asset's ability to deliver its core functions. The consequences of interference with OT or ICT systems can include loss of operational control, reduced situational awareness, delays in response, and increased likelihood of cascading failures.

Given these potential impacts, responsible entities should ensure their CIRMP identifies where such interference could occur and consider implementing appropriate measures to minimise or eliminate this material risk.

In developing their CIRMP, responsible entities should include measures to prevent, detect and respond to these risks. They may consider measures such as system hardening, access controls, network segmentation, monitoring and logging, incident detection capabilities and robust change management processes. These measures support the responsible entity's ability to maintain the integrity and availability of key systems and to respond effectively in the event that interference occurs.

Mitigations such as critical systems segregation and multi-factor authentication may assist responsible entities in addressing these risks. Implementation of these mitigations is required for entities subject to the enhanced CIRMP, however it is recommended that all responsible entities consider these mitigations. See **4.2.3** of Chapter 4 – **Credential compromise hazards** and **5.2.5** of Chapter 5 – **Lateral movement hazards** for more information on these mitigations.

2.2.3.4 Risk arising from the storage, transmission or processing of sensitive operational information outside Australia

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP to minimise or eliminate the material risk of the storage, transmission or processing of sensitive operational information outside Australia (sections 6(d) and 7(1)(c) of the CIRMP Rules and section 8(e) of the TSRMP Rules).

- Sensitive operational information includes:
- layout diagrams
- schematics
- geospatial information
- configuration information
- operational constraints or tolerances information
- data that a reasonable person would consider to be confidential or sensitive about the asset

The impacts of inappropriate storage, transmission or processing of sensitive operational information can be significant. These may include loss of confidentiality, increased exposure to cyber threats, facilitation of malicious activity, or heightened risk of targeted attacks against the asset. In some cases, the compromise of such information may not immediately disrupt operations but could enable future attacks or degrade the overall security posture of the CI asset over time.

In developing their CIRMP, responsible entities should identify where sensitive operational information is stored, transmitted and processed, and assess the risks associated with those arrangements.

Responsible entities should consider the extent to which they retain control over the information, the security measures in place to protect it, and the legal or jurisdictional risks that may apply. Taking a proactive approach to

managing these risks will support the protection of critical information and reduce the likelihood that it could be used to compromise the asset.

Sensitive information is often a key part of carrying out functions in the CI asset. It is often used across the organisation, and as such compromise of sensitive information can have cascading impacts across all hazard vectors and contribute to broader impacts across the CI asset.

Mitigations such as multi-factor authentication may assist responsible entities in addressing these risks. Implementation of this mitigation is required for responsible entities subject to the enhanced CIRMP, however it is recommended that all responsible entities consider this mitigation. See **4.2.3** of Chapter 4 – **Credential compromise hazards**.

2.2.3.5 Risk arising from remote access to operational control or operational monitoring systems of the CI asset

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must seek to minimise or eliminate the material risk of remote access to operational control or operational monitoring systems of the CI asset (sections 6(e) and 7(1)(c) of the CIRMP Rules and section 8(f) of the TSRMP Rules).

Responsible entities should consider the risk that remote access to operational control or monitoring systems for a CI asset can introduce vulnerabilities or reduce the responsible entity's control over those systems. Remote access is often necessary to support operations, maintenance, or vendor activities. However, it can significantly expand the attack surface of the asset if not appropriately managed. This risk is particularly relevant where systems critical to the operation of the asset can be accessed from outside the organisation's secure environment.

Remote access risks arise where individuals - such as employees, contractors or third-party vendors - are able to connect to operational systems from external networks or locations. While this may enable flexibility and efficiency, it can also create opportunities for unauthorised access, particularly if authentication controls are weak, connections are not adequately secured, or access privileges are not tightly managed. For example, an attacker may use compromised user credentials to remotely access a control system or exploit an unsecured remote access pathway to gain entry into internal networks.

In developing their CIRMP, responsible entities should ensure they have appropriate measures in place to manage remote access risks.

Mitigations such as critical systems segregation, multi-factor authentication may assist responsible entities in addressing these risks. Implementation of these mitigations is required for entities subject to the enhanced CIRMP, however it is recommended that all responsible entities consider these mitigations. See **4.2.3** of Chapter 4 – **Credential compromise hazards** and **5.2.5** of Chapter 5 – **Lateral movement hazards** for more information on these mitigations.

2.2.3.6 Risk arising from impacts to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data

Responsible entities for CI assets subject to the baseline or the enhanced CIRMP or the TSRMP must seek to minimise or eliminate the material risk of impacts to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data (sections 6(f) and 7(1)(c) of the CIRMP Rules and section 8(i) of the TSRMP Rules).

Business critical data is defined in section 5 of the SOCI Act and includes information relating to personal data, operational information and risk management processes. See the **glossary** for more detail.

The obligation to establish and maintain a process or system in the CIRMP to minimise or eliminate this material risk may require responsible entities to consider situations beyond a data breach. A material risk may also arise from events such as denial of service attacks or sabotage.

Responsible entities should consider maintaining an inventory of where business critical data is stored within their networks, third-party providers, cloud services, and vendors so they can put in place appropriate controls to manage this material risk.

In addition to identifying where business critical data is stored responsible entities may need to consider how it is managed, including the systems, networks and third parties involved. Entities should consider assessing how disruptions, corruption, unauthorised access or unauthorised disclosure of this data could affect the operation of the asset and implement appropriate measures to manage these risks. This may include data protection controls, access management, system monitoring, and backup and recovery arrangements, which together support the continued availability and reliability of business critical data.

2.2.4 Minimise or eliminate the material risks (enhanced)

Best practice for all responsible entities to consider

CIRMP enhanced – section 6A(1) and (2) of the CIRMP Rules

Responsible entities for CI assets subject to the enhanced CIRMP must minimise or eliminate the following material risks:

- any impairment of the CI asset's functions that could prejudice the social stability, economic stability, national security or defence of Australia
- compromise or impairment of the functions of the CI asset as a result of, or in connection with FOCI;
- offshore or remote access to critical components; and
- offshore or remote access to business critical data.

It is best practice for all responsible entities to consider these material risks. Information on these risks are provided below.

2.2.4.1 Impairment of the CI asset's functions that could prejudice the social stability, economic stability, national security or defence of Australia

The responsible entity must establish and maintain a process or system to – so far as is reasonably practicable - minimise or eliminate the material risks arising from any impairment of the CI asset's functions that could prejudice the social stability, economic stability, national security or defence of Australia (section 6A(2)(a) of the CIRMP Rules).

Impairment is ordinarily defined as to make worse, or alter for the worse.

Prejudice is ordinarily defined as to affect disadvantageously or detrimentally.

National security is defined in section 5 of the SOCI Act as meaning Australia's defence, security or international relations.

Security is defined in section 5 of the SOCI Act as (other than in references to national security). See the **glossary** for this definition.

Security in this context relates to the asset's capability or operational resilience as well as its resilience against national security risks.

International relations is defined in section 5 of the SOCI Act as meaning political, military and economic relations with foreign governments and international organisations.

This material risk intends to capture situations in which the potential impact could extend beyond the CI asset and have broader consequences on Australia. In practical terms, responsible entities should consider whether an impairment to the asset's functions could materially impact Australia's ability to maintain:

- public order and community confidence
- economic activity and financial stability
- national security interests
- defence capability and operations

This is not an exhaustive list, and responsible entities should consider this more broadly in the context of their CI asset.

2.2.4.2 Compromise or impairment of the functions of the CI asset as a result of, or in connection with FOCI

The responsible entity for CI assets subject to the enhanced CIRMP must establish and maintain a process or system in the entity's CIRMP to - as far as reasonably practicable to do so - minimise or eliminate the material risk arising from compromise or impairment of the CI asset's functions as a result of, or in connection with **FOCI** (section 6A(2)(b) of the CIRMP Rules).

It is recommended that responsible entities refer to the Department's **FOCI Risk Assessment Guidance**[1] when assessing whether FOCI may present risks to a CI asset, service provider or supply chain arrangement. The guidance provides a structured approach to identifying FOCI risk, considering potential pathways for foreign direction or influence, and determining appropriate mitigations.

Contract Clauses

Entities are encouraged to consider whether using contract clauses, as part of their contractual arrangements with vendors and other third-parties, may mitigate risks arising as a result of, or in connection with FOCI. Contracts can be an effective mechanism to manage risk from the outset of a procurement or service arrangement because they set clear expectations before access, services or information flows are established. They can define what access a vendor may have, where data may be stored or processed, what security controls must be maintained, how changes in ownership or control must be notified, and what audit, reporting, assurance and termination rights are available to a critical infrastructure entity.

The Department has created a **FOCI Model Contract Clause Bank**[2] to assist in the drafting of clauses for entities.

The model clauses:

- are designed to support a range of procurement activities, including tendering, contracting and contract management;
- can be used for a range of procurements;
- are all optional – responsible entities may select the relevant clauses that they wish to include in their procurement documents based on FOCI risk for that particular project; and
- use the terminology and format of the Commonwealth Contracting Suite (CCS) documentation so that they can be incorporated into CCS procurement documents

Used appropriately, contractual terms can help mitigate FOCI risks by implementing enforceable contractual obligations, supporting ongoing assurance of vendor behaviour, and preserving the responsible entity's ability to respond if risk changes during the life of the contract.

2.2.4.3 Risk arising from offshore or remote access to critical components

The responsible entity for CI assets subject to the enhanced CIRMP must establish and maintain a process or system in the entity's CIRMP to - as far as reasonably practicable to do so - minimise or eliminate the material risk of offshore or remote access to critical components (section 6A(2)(c) of the CIRMP Rules).

This risk seeks to address remote access to critical components that are onshore (such as offshore or onshore parties remotely accessing onshore components), and the risk of offshore access to critical components that are also offshore (such as offshore actors directly accessing critical components which are also offshore).

Remote access

Having a critical component that is remotely located may result in maintenance of systems being conducted via remote access, as opposed to by a same-location worker. Remote access to critical components can increase attack surface by creating pathways by which actors can access critical systems from outside the physical CI environment. If remote access arrangements are inadequately secured it may allow unauthorised parties to exploit vulnerabilities through trusted connections.

Responsible entities are encouraged to document all remote access arrangements to critical components to ensure they are subject to appropriate governance and oversight.

---

[1] https://www.homeaffairs.gov.au/nat-security/files/foci-risk-assessment-guidance-with-appendices.pdf

[2] https://www.homeaffairs.gov.au/nat-security/files/foci-model-contract-clauses.pdf

Offshore access

Entities may make use of offshore staff, contractors or vendors for accessing critical components. This can introduce risk to the CI assets.

Offshore parties may be harder to background check thoroughly. This can be due to having limited access in criminal history, differences in record keeping and identity documents, and jurisdictional limitations preventing appropriate access to information to verify claims. As a result, it may be difficult to ascertain suitability and trustworthiness for accessing important systems and data. In addition, it may be difficult to gain proper assurance of the security posture of devices these parties use for obtaining access to control systems or business critical data. The devices they use may therefore be more susceptible to compromise for these or other reasons (such as due to opaque supply chains).

Individuals based offshore may also be particularly prone to influence from foreign nation-states or other parties in ways that are detrimental to the security of a CI asset.

Entities are encouraged to document all remote and offshore access arrangements, including associated risks and controls, and ensure these are subject to appropriate governance, oversight, and periodic review. This should include clear accountability for approving, monitoring, and revoking access, as well as assurance activities (such as audits, testing) to validate the effectiveness of controls.

Responsible entities are required to undertake suitability assessments for critical workers (as per **6.2.5** of Chapter 6 – **Personnel hazards**) which will assist in mitigating this risk. Additionally, responsible entities subject to the enhanced CIRMP are required to implement phishing resistant multi-factor authentication (see **4.2.3** of Chapter 4 – **Credential compromise hazards**) and critical system segregation (see **5.2.5** of Chapter 5 – **Lateral movement hazards**). Implementation of these mitigations is best practice for all responsible entities.

2.2.4.4 Risk arising from offshore or remote access to critical components

The responsible entity for CI assets subject to the enhanced CIRMP must establish and maintain a process or system in the entity's CIRMP to - as far as reasonably practicable to do so - minimise or eliminate the material risk of offshore or remote access to business critical data (section 6A(2)(d) of the CIRMP Rules).

This risk seeks to address both remote access to business critical data that is stored onshore (such as offshore or onshore actors remotely accessing business critical data), and offshore access to business critical data that is also stored offshore (such as offshore actors directly accessing offshore business critical data stored offshore).

Business critical data is defined in section 5 of the SOCI Act, see the **glossary**.

Entities should identify and assess risks arising from offshore or remote access to business critical data associated with their CI asset. This includes any storage, processing, transmission, or access to sensitive or operational data from locations outside the organisation's direct control, including offshore jurisdictions and third-party environments.

For example, remote administration of operational systems or offshore data processing arrangements may increase the likelihood of unauthorised access or complicate incident response efforts.

Responsible entities are required to undertake suitability assessments for critical workers (as per **6.2.5** of Chapter 6 – **Personnel hazards**) which will assist in mitigating this risk. Additionally, responsible entities subject to the enhanced CIRMP are required to implement phishing resistant multi-factor authentication (see **4.2.3** of Chapter 4 – **Credential compromise hazards**) and critical system segregation (see **5.2.5** of Chapter 5 – **Lateral movement hazards**). Implementation of these mitigations is best practice for all responsible entities.



2.3 Best practice for identifying and mitigating risks

This section provides guidance on best practice mitigations for risks associated with all hazards. Responsible entities should consider whether these mitigations will assist them in meeting their obligation to establish and maintain a process or system in the entity's CIRMP to minimise or eliminate material risks, and mitigate the relevant impact of each hazard on the asset (section 7(1)(c) of the CIRMP Rules). The guidance does not comprehensively cover all possible mitigations or risks. The responsible entity must consider additional mitigations as required to address all potential material risks to the CI asset.

2.3.1 Material risks for consideration

Responsible entities must mitigate against the specified material risks in the CIRMP Rules, however they should also consider other possible material risks.

Below are some suggested material risks for consideration. There may be other material risks that are not included in this guidance. It is the responsibility of the responsible entity to identify, eliminate, and minimise these material risks.

Risk Category	Description
Governance and organisational capability risks	Responsible entities may consider risks arising from weaknesses in governance, leadership, or organisational capability that may affect their ability to manage security and resilience. For example, unclear accountability for risk management, insufficient resourcing, or ineffective decision-making processes may reduce the responsible entity's ability to identify, respond to or recover from disruptions. These risks may not directly affect physical systems but can significantly impact the responsible entity's overall resilience.
Single points of failure and concentration risks	Entities may consider risks created by over-reliance on a single system, supplier, site, or capability. A failure in a single critical dependency can lead to disproportionate disruption if there are no viable alternatives or redundancy arrangements in place. For example, reliance on a single data centre, a sole supplier of a critical component, or one operational control location may create vulnerabilities that amplify the impact of an incident.
Interdependency and cascading risks	Responsible entities may consider the risk that disruption to another system, asset or sector may impact their own operations. CI assets are interconnected, and failures can cascade across sectors. For example, loss of telecommunications may affect energy system monitoring, or disruption to transport networks may affect supply chain delivery. These risks may not originate within the asset itself but can still have a material impact.
Change and transition risks	Entities may consider risks arising from periods of change, including system upgrades, digital transformation, infrastructure expansion, or organisational restructuring. These periods can introduce vulnerabilities due to incomplete controls, system misconfigurations, or reduced oversight. For example, implementation of new technology or migration to cloud systems may create temporary exposure if not properly managed.

2.3.2 Treating risk – mitigations and controls

The mitigations for all hazard risks are provided throughout all chapters of this guidance document. By having a robust CIRMP, that considers and implements mitigations across all hazard vectors, responsible entities will address the risks listed in this chapter. Having appropriate governance and control mechanisms on maintaining the CIRMP will ensure these mitigations are fit for purpose and support the security of the CI asset.

2.4 Worked example – CIRMP entry

Field	Example Response
Hazard	Unauthorised or unmanaged offshore access to critical systems
Asset(s) / Site	Network Operations Centre (NOC) – Site B (coordinates delivery of essential services, including monitoring and management systems
Scenario	An offshore service provider is granted access to maintain operational systems. Access controls, monitoring, or contractual restrictions are insufficiently defined or enforced, resulting in elevated, persistent, or inappropriate access beyond operational need.
Why this is material	Offshore access can introduce exposure to risk through external access to systems or data access outside direct operational oversight.
Relevant impact mapping	**Integrity:** unauthorised changes to system configuration, patching, or operational processes through offshore access pathways. **Confidentiality:** exposure of sensitive operational information (system architecture, credentials, incident data) through offshore access.
Evidence supporting likelihood	• Offshore access arrangements documented, including systems accessed and access methods (Completed — Mar 2026). • Access logs and monitoring reports identify frequency and scope of remote sessions (Ongoing review — from Jan 2026). • Internal audit findings identify gaps in access governance, monitoring, or third-party controls (In progress — due Aug 2026).
Key dependencies / interdependencies ***(Include here the cascading impact that may result from the realisation of the hazards)***	• Offshore service providers or remote personnel supporting monitoring, maintenance, or incident response. • Identity and access management systems controlling authentication and permissions. • Network architecture enabling remote connectivity (VPNs, gateways, remote access platforms).
Controls — Preparedness	• Defined process for approving, provisioning, and reviewing offshore or remote access (Implemented — Mar 2026). • Risk assessment process applied prior to granting offshore or remote access (Implemented — May 2026).
Controls — Prevent / minimise likelihood	• Restrict offshore or remote access to approved methods (such as managed VPN, secure gateway); prohibit uncontrolled access pathways (Implemented — Jan 2026). • Enforce least-privilege access, time-bound access, and individual user accounts; prohibit shared credentials (Implemented — Jan 2026). • Require multi-factor authentication and device security controls for offshore or remote connections (Implemented — Feb 2026). • Implement session monitoring, logging, and routine review of offshore or remote access activity (Implemented — Jan 2026). • Define contractual controls for third-party offshore access where applicable, including audit rights and security requirements (In progress — Sep 2026).
Controls — Impact mitigation	• Segregate critical systems and limit offshore or remote access to controlled environments where feasible. • Maintain real-time monitoring and alerting for anomalous offshore access behaviour. • Maintain incident response procedures specific to offshore or remote access compromise scenarios. • Enable rapid revocation of access (accounts, sessions, credentials) in response to suspected compromise.

Owners / status / timeframes	• Offshore and remote access governance — Head of Cyber Security (implemented, quarterly review) • Third-party access controls — Vendor Management Lead (in progress; Sep 2026). • Monitoring and logging — Security Operations Centre Lead (implemented; uplift Oct 2026).
Residual risk and acceptance	Residual risk assessed as medium due to continued reliance on offshore access pathways and associated visibility and control limitations. Risk accepted by Risk Committee (Jun 2026), subject to ongoing monitoring, periodic access reviews, and continued uplift of access assurance controls.
Review cadence / triggers	Review annually and trigger review after: • onboarding or offboarding of offshore providers or remote users with system access • changes to remote access architecture or authentication methods • significant cyber security incidents involving offshore or remote access pathways • material changes to service delivery arrangements or operating environment
Supporting material	• Offshore and remote access policy and procedures • Third-party risk assessments and contractual agreements (where applicable) • Access control and identity management documentation • Remote access logs and monitoring reports • Incident response plans and scenario exercise outputs

Table of contents: Chapter 3

3.1 Obligations for managing cyber and information security hazards 32
3.2 Meeting the obligations in practice 34
3.2.1 Minimise or eliminate a material risk, and mitigate the relevant impact 34
3.2.2 Comply with a cyber security framework 35
3.2.2.1 Alternative cyber security frameworks 36
3.2.2.2 Cyber security frameworks – tailoring implementation of security controls 41
3.2.3 Minimise or eliminate specified material risks 42
3.2.4 Risk arising from failure to patch or update operating or security systems in a timely manner 42
3.2.4.1 Risk arising from failure to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued 43
3.2.4.2 Risk arising from deployment or hosting of advanced, novel and emerging technology 43
3.2.4.3 Risk arising from the use of advanced, novel and emerging technology against the asset 44
3.3 Best practice for identifying and mitigating risks 45
3.3.1 Material risks for consideration 45
3.3.2 Treating risk – mitigations and controls 46
3.3.2.1 Patching and updating in critical infrastructure environments 46
3.3.2.2 Managing the use of legacy systems and unsupported or obsolete hardware, software or critical components 47
3.3.2.3 Managing risks associated with novel, advanced and emerging technologies 47
3.3.2.4 Cyber threat intelligence sharing 49
3.4 Worked example – CIRMP Entry 52

3. Cyber and information security hazards

Cyber systems and networks underpin the operation of critical infrastructure. They face constant and evolving threats from malicious actors, including state-sponsored attacks, criminal groups, and insider threats. The Australian Signals Directorate's (ASD) Australian Cyber Security Centre's (ACSC) **Annual Cyber Threat Report for 2025-26**[3] reported that critical infrastructure incidents made up 10% of all incidents. A successful breach of a CI asset can lead to a range of consequences including potential data exfiltration, reduced operational performance or shutdowns, and cascading im pacts across sectors and communities. It can also result in harm to people, the environment or equipment. For CI assets, these consequences can be detrimental to the economic security, national security, and defence of Australia.

Managing cyber and information security hazards is essential to protecting the continuity and resilience of Australia's CI assets.

3.1 Obligations for managing cyber and information security hazards

The table below outlines the obligations in the CIRMP Rules in relation to cyber and information security hazards. It outlines whether the obligations apply to entities subject to the baseline and/or enhanced CIRMP requirements and/or TSRMP requirements. The obligations are expanded on later in this chapter.



[3] https://www.cyber.gov.au/publication/annual-cyber-threat-report-2025-26

Cyber and information security hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
A responsible entity for a CI asset must establish and maintain a process or system to – so far as reasonably practicable to do so – minimise or eliminate any material risk of a cyber and information security hazard occurring and mitigate the relevant impact of a cyber and information security hazard on the CI asset.	s 8(2)	s 8(2)	s 11(2)
A responsible entity for a CI asset must establish and maintain a process or system to comply with a framework contained in a document specified in the CIRMP (and if applicable – the TSRMP) Rules, and meet any relevant conditions mentioned in the Rules for that document. The responsible entity must otherwise establish and maintain a process or system in the entity's CIRMP to comply with a framework that is equivalent to a framework contained in a document specified in the CIRMP (and if applicable – the TSRMP) Rules, including any relevant conditions mentioned in the Rules for that document.	s 8(4) s 8(5)	s 8A(3) s 8A(4)	s 11(3) s 11(4) s 11(5)
A responsible entity for a CI asset subject to the enhanced CIRMP must establish and maintain a process or system in the entity's CIRMP to – so far as it is reasonably practicable to do so – minimise or eliminate each of the following material risks: (a) Failure to patch or update operating or security systems in a timely manner; (b) Failure to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued; (c) Deployment or hosting of advanced, novel or emerging technologies that could prejudice the availability, integrity, reliability or confidentiality of the CI asset; and (d) Use of advanced, novel or emerging technologies against the asset, in a manner that could prejudice the availability, integrity, reliability or confidentiality of the CI asset.		s 8A(2)	

Timeframes for compliance are explained in Chapter 1 – **Introduction to the critical infrastructure risk management program (CIRMP)** at **1.5**

3.2 Meeting the obligations in practice

3.2.1 Minimise or eliminate a material risk, and mitigate the relevant impact

CIRMP baseline – section 8(2) of the CIRMP Rules

CIRMP enhanced – section 8(2) of the CIRMP Rules

TSRMP – section 11(2) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must establish and maintain a process or system, as far as it is reasonably practicable to do so, to minimise or eliminate any material risk of a cyber and information security hazard occurring and mitigate the relevant impact of a cyber and information security hazard on a CI asset.

There are no specified material risks in section 8 of the CIRMP Rules, or section 11 of the TSRMP Rules. The material risks that are listed in section 6 and 6A of the CIRMP Rules are discussed in Chapter 2 – **All hazards**.

This chapter outlines the material risks for responsible entities subject to the enhanced CIRMP, as well as suggested material risks that are specific to cyber and information security hazards. It also details potential mitigations. Refer to **2.2.4** of Chapter 2 – **All hazards** for enhanced material risks and **2.3.1** for suggested material risks.



3.2.2 Comply with a cyber security framework

CIRMP baseline – section 8(4) and 8(5) of the CIRMP Rules

CIRMP enhanced – section 8A(3) and 8A(4) of the CIRMP Rules

TSRMP – section 11(3), (4), and (5) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must comply with a cyber security framework listed in the CIRMP Rules or an alternative framework that is equivalent to a listed framework. For information on the TSRMP requirements see the **Guidance for Responsible Entities for Critical Telecommunications Assets**. The listed frameworks and associated maturity levels that entities must meet for certain listed frameworks are outlined below:

Framework	Baseline CIRMP Maturity Level
Australian Standard AS ISO/IEC 27001:2015.	
Essential Eight Maturity [4]Model – published by the Australian Signals Directorate.	If any entity elects to comply with this framework, they must meet Maturity Level 1.
Framework for Improving Critical Infrastructure Cybersecurity - published by the National Institute of Standards and Technology of the United States of America.	
Cybersecurity Capability Maturity Model – published by the Department of Energy of the United States of America.	If an entity elects to comply with this framework they must meet Maturity Indicator Level 1.
The 2020-21 AESCSF Framework Core – published by Australian Energy Market Operator Limited (ACN 072 010 327).	If an entity elects to comply with this framework they must meet Security Profile 1.
Framework	**Enhanced CIRMP** **Maturity Level**
Australian Standard AS ISO/IEC 27001:2023.	
****Essential Eight Maturity Model*** – published by the Australian Signals Directorate.	If any entity elects to comply with this framework, they must meet Maturity Level 2.
The NIST Cybersecurity Framework (CSF) 2.0 – published by the National Institute of Standards and Technology of the United States of America.	
****Cybersecurity Capability Maturity Model (Version 2.1) –*** published by the Department of Energy of the United States of America.	If an entity elects to comply with this framework they must meet Maturity Indicator Level 2.
****The 2023 AESCSF Framework Core*** – published by Australian Energy Market Operator Limited (ACN 072 010 327).	If an entity elects to comply with this framework they must meet Security Profile 2.

If a responsible entity does not comply with a framework listed above, they must comply with an alternative cyber security framework that is **equivalent** to a listed framework (see below for further explanation).

[4] The Essential Eight Maturity Model will evolve to the Essential Series following publication in October 2026. The CIRMP Rules have not yet been updated to reflect this. Responsible entities are encouraged to consider transitioning to the Essential Series following its publication. The Essential Series, if implemented in full, is considered an equivalent cyber security framework.

Responsible entities that are subject to the enhanced CIRMP, and are complying with an alternative framework that is not a listed framework, must ensure their framework is equivalent to a listed framework marked with an asterisk (*). Additionally, they must assess the equivalency of the framework by the security outcomes achieved by maturity level 2, maturity indicator level 2, or security profile 2 (as applicable) of the listed framework.

3.2.2.1 Alternative cyber security frameworks

The responsible entity can elect to use a cyber security framework that is **equivalent** to one of the listed frameworks. To comply, the responsible entity will have to determine if the equivalent framework is appropriate to address the risks threatening the CI assets, and whether it has the same or similar controls and mitigations as the prescribed frameworks at the required maturity level.

For CI assets subject to the enhanced CIRMP, the responsible entity is expected to comply with Maturity Level 2 of the chosen framework. Where an equivalent framework that is not listed is chosen, or a framework that does not have a specified Maturity Level 2, the responsible entity should outline steps taken in the CIRMP to make the cyber program equivalent to Maturity Level 2 of a prescribed framework. This may require the implementation of more rigorous or additional security controls than the chosen framework describes.

The Essential Series published by the Australian Signals Directorate is considered to be an equivalent cyber security framework for the purposes of section 8(5) and 8A(4).

Selecting an alternative cyber security framework

In selecting an equivalent framework, a responsible entity may consider:

- **Framework scope** - to effectively minimise or eliminate as broad a range of material risks as possible, consider adopting a framework that takes a holistic approach to implementing cyber security controls. Frameworks with a narrow focus (either in control or technology focus) or too general in their approach may necessitate the implementation of additional controls.
- **Currency of framework** – frameworks that are significantly dated may not account for recent threats and technology trends. Selecting a framework that is dated would require clear justification and the potential implementation of additional controls to account for emerging threat trends and attack vectors not covered or contemplated by the framework. Consideration should be given to what adversary tradecraft needs to be protected against and whether the proposed framework provides suitable mitigations for such tradecraft.
- **Appropriateness of framework** – consider whether the proposed framework is suitable for the sensitivity or classification of data an entity is expected to protect and is compatible with Australian protective security policy and cyber security guidance. Some frameworks only endorse assessors from the country of origin of the framework or are subject to influence of the country of origin.
- **Appropriateness for technology environment and threat environment** – consider the technology environments and threat profiles when selecting an alternative framework. For example, for CI assets with significant OT, frameworks with little guidance on adapting controls to these environments may be problematic. The responsible entity would need to select an alternative framework or have a detailed plan for how controls will be adapted in the framework to suit the environment.
- **Prior adoption and considerations of expediency** - considerations of expediency, such as the cost of implementing or certification of a framework, or previous adoption by a responsible entity, may be factored into the decision as to what framework is selected. However, this factor should not be the sole determinant for selecting a framework and should not be used by a responsible entity to avoid implementing controls that are fundamental to managing risks.

This is not a comprehensive list of considerations. Responsible entities are best placed to understand the nuance of their CI asset, and there may be other considerations that are relevant to assessment of selecting a framework.

Assessing equivalency of alternative cyber security frameworks

Responsible entities that elect to comply with a framework that is not listed in the tables above for baseline and enhanced entities (section 8(4) for baseline entities and section 8A(3) for enhanced entities of the CIRMP Rules) are required to comply with a cyber security framework that is equivalent to a listed framework.

In practice, this means the responsible entity's framework must be, at a minimum, equivalent to only one of the frameworks. There is no requirement that it be equivalent to *all* listed frameworks.

The steps outlined below seek to assist responsible entities in assessing an alternative framework that they are already complying with.

Step 1. Identify the scope of the CI asset

When applying the cyber security framework, the responsible entity should determine the most appropriate scope for the framework. The scope establishes which systems, technologies, information assets, and supporting processes are subject to the framework and its controls.

For the purposes of the CIRMP, responsible entities should consider the scope based on the operational context of the CI asset. This should include consideration of all cyber-enabled systems and dependencies that support the delivery of the critical services. It is recommended that responsible entities identify and consider:

- information technology systems
- operational technology systems
- information assets required for the operation, management, or recovery of the CI asset
- external dependencies and third-party services (such as cloud service providers and managed service providers)
- communications systems
- interconnections and interfaces between systems, both internally and externally.

Responsible entities should seek to apply the framework as broadly as reasonably practicable across the cyber systems that support the CI asset. Where systems or services contribute to the delivery, maintenance, or recovery of the proper function of the CI asset, those systems should be considered within scope. If they are not included, responsible entities should document in their CIRMP why the systems or services have been excluded. Any exclusions should be risk-informed and justified. The boundaries of the scope should be documented appropriately and reviewed regularly. It is also best practice to clearly outline who is accountable for this review process and for any accepted risk.

Step 2. Identify the most appropriate listed framework that addresses the assets operational context

The listed cyber security frameworks have different objectives, scopes and areas of focus. While each framework seeks to strengthen cyber security outcomes, they do not all address the same technologies, operating environments or risk profiles to the same level of detail.

The equivalency of the alternative framework only needs to be demonstrated against one of the listed frameworks. When selecting the framework to assess equivalency against, responsible entities should select the most appropriate framework, based on the operational context of the CI asset. The listed frameworks vary in their approach.

- Some frameworks provide broad, organisation wide cyber security governance and risk management (such as ISO 27001/ISO 27002 and the NIST Cybersecurity Framework).
- Some frameworks contain controls and guidance that are tailored to particular sectors or operational environments (such as the Australian Energy Sector Cyber Security Framework).
- Some frameworks use maturity-based approaches to assess and improve cyber security capabilities (such as the Essential Eight Maturity Model and the Cybersecurity Capability Maturity Model)

Responsible entities should select the framework that provides the most **relevant** comparison for the CI asset. For example, where a CI asset relies heavily on OT a framework that specifically considers these environments is more appropriate than a framework that focuses on primarily IT environments. It is best practice to ensure the CI asset has an appropriate IT framework and OT framework, which may require different frameworks across the CI asset.

Identifying the most appropriate listed framework to undertake a comparison will ensure that a meaningful assessment of equivalency is conducted and the risk environment faced by the CI asset is being appropriately mitigated against.

Step 3. Identify the key security outcomes achieved by the listed framework

Once the responsible entity has identified the listed framework that is most relevant to the operational context of the CI asset, they should determine the security outcomes that the framework achieves. This assessment should focus on outcomes rather than controls, because cyber security frameworks often vary greatly in their structure and approach but generally achieve the same security outcomes.

Responsible entities should consider the selected framework as a whole and identify the key outcomes it seeks to achieve. Some frameworks define outcomes through controls, while others describe capabilities or security objectives that can be achieved through different approaches. The responsible entity should focus on the practical security outcome achieved by the framework.

The responsible entity should consider the framework they selected in Step 2 and determine what the outcomes are for that framework.

For example, the NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1 (baseline framework requirement) is organised around core functions that describe desired cyber security outcomes. Within each function there are categories and subcategories that describe cybersecurity outcomes. These categories and subcategories do not prescribe exactly how those outcomes must be achieved.

Step 4. Determine whether the alternative framework achieves the same outcomes

Once the responsible entity has determined what security outcomes are achieved in the selected listed framework, they should then consider whether the alternative framework is achieving the same outcomes.

For example, if the listed framework achieves a defined security outcome (such as identifying and assessing suppliers using a cyber supply chain risk management process) through specific controls or practices, the responsible entity must ensure that the same practical security outcome is achieved, whether through the same controls or through other measures that collectively deliver an equivalent outcome.

The responsible entity should consider **all** the outcomes achieved in the selected listed framework. The alternative framework should also achieve all these security outcomes. The alternative framework may achieve additional security outcomes, however this is not required.

Step 5. Implement compensating measures to address any gaps

If the alternative security framework does not address all the security outcomes of the listed framework, the responsible entity must introduce additional measures to achieve the security outcomes achieved through the listed framework.

These additional measures may form part of the cyber security framework (such as the responsible entity is using an in-house cyber security framework so additional measures will be included in the framework) or they may be in addition to the cyber security framework (such as the responsible entity is using a framework that is prescribed by another agency, and as such they introduce additional measures which are to supplement the prescribed framework).



Examples of equivalence

Below is an example of a hypothetical alternative framework (referred to as AF) compared with the NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1.

NIST Security Outcome	Alternate framework control/s	Assessment	Additional control / variation needed
Incident response plan is executed during or after an incident.	AF-IR-01 Incident Response Procedure: requires the organisation to maintain and execute an incident response procedure.	AF-IR-01 achieves the same security outcome. They require the incident response plan to be executed during an incident.	No additional measures required
Suppliers and third-party partners of information systems, components and services are identified, prioritised and assessed using a cyber supply chain risk assessment process.	AF-TPR-01 Supplier Register: requires the organisation to maintain a list of suppliers.	AF-TPR-01 achieves majority of the security outcome because they require suppliers to be identified. However, they do not confirm that suppliers are prioritised or assessed using a cyber supply chain risk assessment process.	An additional measure is required to achieve the same outcome. Introduce AF-TPR-03 Supplier Cyber Risk Assessment and Criticality Rating to meet the same outcome.
Backups of information are conducted, maintained and tested.	AF-DATA-01 Records Retention Procedure: requires important business records to be retained for defined periods.	AF-DATA-01 may not meet the security outcome because retaining records is not the same as conducting, maintaining and testing backups. The control may support information governance, but it does not address backup creation, backup protection, restore testing or recovery assurance.	Additional controls are required to meet the NIST backup outcome. Add controls for scheduled backups, backup monitoring, backup protection, restore testing, backup ownership, recovery objectives and evidence that backups for systems supporting the CI asset are maintained and tested.

Entities using listed framework with maturity condition

The Australian Standard AS ISO/IEC 27001:2023 and the NIST Cybersecurity Framework (CSF) 2.0 do not list required maturity levels. Responsible entities who are adopting these frameworks are encouraged to ensure that their cyber security framework is equivalent to Maturity Level 2 or Security Profile 2 of the listed frameworks that include maturity of security levels.

Responsible entities should be mindful of the operational context of the CI asset, and the extent to which their cyber security framework addresses the security risks faced by the CI asset. For example, a responsible entity of an asset with significant amounts of OT and Supervisory Control and Data Acquisition (SCADA) who has elected to comply with AS ISO/IEC 27001:2023 should consider whether the controls implemented are appropriate both in nature and in coverage of their OT environment. In this circumstance the responsible entity would be strongly encouraged to consider and implement controls found in more OT focused frameworks, such as the 2023 AESCSF Framework Core, to supplement their security.

The table below provides examples of how ISO 27001 controls may be assessed against selected AESCSF SP2 security outcomes. The purpose is to assess whether ISO 27001 achieves the same practical security outcomes as the AESCSF SP2 despite their different structures. Where ISO controls only partially achieve the outcome, additional controls or control variations may be required. Where there is no direct match, the responsible entity should ensure that the control achieves the same security outcome.

AESCSF SP2 Security Outcome	ISO 27001 control/s	Assessment	Additional control / variation needed
Incident response processes are established, executed and improved after cyber security events or incidents.	A.5.24: Information security incident management planning and preparation A.5.26: Response to information security incidents A.5.27: Learning from information security incidents	ISO controls A.5.24, A.5.26 and A.5.27 achieve the same security outcome. They require incident planning, response, and post-incident learning. Together, these controls address the AESCSF SP2 outcome of having an incident response process that can be activated, performed and improved.	No additional control is required.
Assets, configurations and changes are identified, managed and controlled across systems supporting the critical infrastructure asset.	A.5.9: Inventory of information and other associated assets A.8.9: Configuration management A.8.32: Change management	ISO controls A.5.9, A.8.9 and A.8.32 achieve the majority of the security outcome. They require asset inventory, configuration management and controlled change management. However, they may not fully meet the AESCSF SP2 outcome unless the controls are extended to the critical infrastructure asset environment, including operational technology, critical system dependencies, configuration baselines and change impacts to operational services. Additional control AESCSF-ACCM-01 Critical Asset and Configuration Management is needed to meet the same outcome.	Add or vary controls to require an asset configuration register.

AESCSF SP2 practices and anti-patterns are specifically assessed, with required practices present and required anti-patterns absent.	ISO 27001 has controls for governance, risk assessment, internal audit, management review and continual improvement, such as clauses 6, 9 and 10, but no direct Annex A control that specifically requires AESCSF SP2 practice/anti-pattern assessment.	ISO 27001 does not meet this AESCSF specific outcome by itself. ISO requires an ISMS, risk assessment, treatment, monitoring and improvement, but it does not require the organisation to assess itself against AESCSF SP2 practices and anti-patterns. AESCSF SP2 specifically requires all SP1 and SP2 practices and anti-patterns to be attained or absent, so an ISO-certified ISMS alone may not prove this outcome.	Add a specific AESCSF SP2 Assessment Control requiring the organisation to map ISO controls to each applicable AESCSF SP2 practice and anti-pattern, record whether each practice is attained, confirm anti-patterns are absent, assign owners, collect evidence and track remediation.

3.2.2.2 Cyber security frameworks – tailoring implementation of security controls

The listed or equivalent cyber security frameworks may include general guidance on implementing controls. The responsible entity should consider how to implement security measures in a way that is appropriately adapted to the relevant environment. For example, significant amounts of OT within a CI asset may require nuanced implementation of controls which may not be covered in detail in the selected framework.

Some examples of controls that may be implemented by a responsible entity are provided below. This is not a comprehensive list and will depend on the nature of the responsible entity and CI asset.

Patching

Timely patching of vulnerabilities can be challenging in critical infrastructure environments due to operational complexities and uptime requirements. This may necessitate the use of compensating controls. This is discussed further in **3.3.2.1**.

Backup and recovery

Backup and recovery processes are important but can prove challenging to implement. Undertaking backups may degrade or interfere with IT/OT system or device uptime. Even if this is for a short duration, it may be unacceptable for CI assets. Similarly, the restoration of backups onto OT devices such as programmable logic controllers, safety systems and human-machine interfaces may require validation and testing (potentially with vendor involvement) and compliance with rigorous change management processes. Having redundancy processes and systems in place to facilitate effective backup and recovery may be necessary in these circumstances.

Compatibility with 'black-start' processes

Some CI assets – such as critical energy assets – may have restart and recovery procedures in place after a complete or partial shutdown (in case of scenarios such as a grid-wide outage). In this context, any security measures used by the asset should be carefully selected to ensure they do not interfere with these recovery processes and that contingency measures are in place while operations are in a degraded state.

For example, security tools should fail or revert to contingency operations rather than blocking system functionality in the event of degraded communications that prevents connection with the cloud (Security Information and Event Management (SIEM) tools revert temporarily to local or offline logging and Endpoint Detection and Response (EDR) tools revert to offline mode). Similarly, where a cloud-based authentication service is used, contingencies could include the temporary reversion to the use of an alternative on-premises authentication mechanism for critical OT systems and devices or the use of pre-provisioned emergency local administrative credentials.

Supply chain vetting

In many organisations, supply chain risk assessment processes typically apply scrutiny to vendors based on them meeting specific thresholds (such as the size of the engagement with the vendor or their operational significance to the organisation). However, critical infrastructure environments may require additional rigour.

For example, the use of legacy communication protocols by some OT devices may result in messages (such as critical device control broadcasts) being sent to all other systems and devices connected to the same network. Any compromised devices, components or software – regardless of size or perceived significance – can enable a malicious party to monitor activities within the environment or pre-position themselves for future cyber attacks.

The use of rigorous supply chain vetting processes is vital in the context of managing cyber hazards. Additionally responsible entities are obligated to manage supply chain hazards, as detailed in Chapter 7 – **Supply chain hazards**.

Effective segregation of OT environments

Adequate segregation of OT networks and authentication mechanisms from IT networks reduces the risk of a compromise in one part of an environment enabling lateral movement of a hostile actor to key operational systems.

Specific considerations for implementing effective segregation of networks in a critical infrastructure context is covered in more detail in Chapter 5 – **Lateral movement hazards**.

Tailored cyber awareness training

Security awareness training is important for all organisations and should be tailored to the specific operational context of a CI asset. Ensuring all personnel receive targeted training and operate within a culture that promotes cyber security vigilance in OT environments is essential.

Incident response plans and procedures

The development of documented incident response plans and scenario-based incident playbooks, as well as processes to test their effectiveness (such as tabletop exercises), is a fundamental part of any effective cyber security program. While the responsible entity may already have general incident response documentation and processes, it is vital that these are integrated with OT-specific incident response processes and scenarios, as well as broader organisational crisis management and business continuity plans. Further, OT-specific response and recovery processes should be developed and regularly reviewed in lockstep with relevant operational staff (such as process engineers) to ensure their ongoing accuracy and efficacy.

3.2.3 Minimise or eliminate specified material risks

Best practice for all responsible entities to consider

CIRMP enhanced – section 8A(2) of the CIRMP Rules

Responsible entities for CI assets subject to the enhanced CIRMP are required to establish and maintain a process in their CIRMP to – so far as it is reasonably practicable – minimise or eliminate the following material risks:

- Failure to patch or update operating or security systems in a timely manner.
- Failure to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued.
- Deployment or hosting of advanced, novel or emerging technology in a manner that could prejudice the availability, integrity, reliability or confidentiality of the CI asset.
- Use of advanced, novel or emerging technologies against the asset, in a manner that could prejudice the availability, integrity, reliability or confidentiality of the CI asset.

It is best practice for all responsible entities to consider these material risks. Information on these risks are provided below.

3.2.4 Risk arising from failure to patch or update operating or security systems in a timely manner

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain a process in their CIRMP to – so far as it is reasonably practicable – minimise or eliminate the material risks arising from failure to patch or update operating or security systems in a timely manner (section 8A(2)(a) of the CIRMP Rules).

Unpatched vulnerabilities in devices, systems and software provide attackers with opportunities to exploit known security weaknesses. Out of date software can mean new features or enhancements that help address emerging security threats are not available. This can lead to unauthorised access to systems, theft of sensitive data, or installation of malicious software within CI assets.

Vulnerabilities in operating systems can be targeted by malicious actors within a short timeframe of being identified. This can provide a platform for attackers to move laterally within environments, pre-position for future attacks or disrupt, sabotage, or interfere with the safe and effective operation of the CI asset.

If the function of these security systems is compromised due to the exploitation of unpatched vulnerabilities, the ability of the responsible entity to detect and respond to a security breach promptly may be diminished. Moreover, these systems are typically given highly privileged access within organisations (for example, Endpoint Detection and Response (EDR) software may be installed on most systems and Security Information and Event Management (SIEM) tools can provide visibility of activity across technology environments). This can provide attackers with a broader level of understanding and potential control of systems and networks.

For information on how to patch and update in a CI environment see **3.3.2.1** of this chapter. This also includes information on what timely patching looks like.

3.2.4.1 Risk arising from failure to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain a process in their CIRMP to – so far as it is reasonably practicable – minimise or eliminate the material risks arising from failure to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued (section 8A(2)(b) of the CIRMP Rules).

Legacy systems and unsupported or obsolete technology may not have patches available to address security vulnerabilities, providing an ongoing window of opportunity for exploitation. Malicious actors may use these vulnerabilities to gain a foothold in the environment and move laterally across to other systems, devices and networks. This may enable them to pre-position for future attacks or disrupt, sabotage, or interfere with the safe and effective operation of CI assets.

Legacy or unsupported systems, components or technology can also create other risks:

- Legacy devices may use insecure communication protocols, enabling eavesdropping, spoofing or replay attacks.
- Redundant systems, components or technology create an expanded potential attack surface that can be targeted.
- Ageing hardware may be prone to unpredictable failures, leading to downtime or operational faults.
- Legacy systems often fail to integrate with modern security mechanisms, such as MFA and endpoint detection and response tools.
- Obsolescence may mean there are fewer staff available who understand the relevant components or technology – this can exacerbate training and maintenance costs and increase the length of any downtime caused by failures.

For information on mitigations for managing legacy system use, see **3.3.2.2** of this chapter.

3.2.4.2 Risk arising from deployment or hosting of advanced, novel and emerging technology

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain a process in their CIRMP to – so far as it is reasonably practicable – minimise or eliminate the material risks arising from deployment or hosting of advanced, novel and emerging technology in a manner that could prejudice the availability, integrity, reliability or confidentiality of the CI asset (section 8A(2)(c) of the CIRMP Rules).

The use of advanced, novel and emerging technologies in CI assets can introduce potential risks which responsible entities should consider and appropriately manage. Advanced, novel and emerging technology may include artificial intelligence, quantum computing, or quantum cryptography. This list is not exclusive, and entities should consider beyond the technologies listed here.

For example, these technologies may have an unproven track record in critical infrastructure environments, meaning reliability may be questionable and there are potential risks to the safety and proper functioning of CI assets. Using these technologies may also mean the process for resolving any failures or incidents arising from their use is more complex, potentially extending the time taken to restore normal operations.

Supply chains for these technologies may be unfamiliar and opaque. The maturity of vendors may not be well understood and the security of associated software or hardware may be difficult to assess.

For information on mitigations for material risks see **3.3.2** of this chapter.

3.2.4.3 Risk arising from the use of advanced, novel and emerging technology against the asset

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain a process in their CIRMP to – so far as it is reasonably practicable – minimise or eliminate the material risks arising from the use of advanced, novel and emerging technology against the asset, in a manner that could prejudice availability, integrity, reliability or confidentiality of the CI asset (section 8A(2)(d) of the CIRMP Rules).

Advanced, novel and emerging technologies may be used by malicious actors to target and attempt to compromise CI assets using previously unforeseen attack paths. They can enable cyber adversaries to bypass existing controls, or scale attacks at a pace which makes identification and interception of attacks difficult.

Emerging technologies can also be used to increase the precision and persistence of attacks. Malicious actors may employ these technologies to tailor attacks to specific asset configurations or maintain a prolonged presence within environments to achieve delayed or cascading impacts. This enables attacks that are difficult to detect at initiation but are designed to amplify consequences across systems.

AI models are also now able to identify previously unknown vulnerabilities in software packages at scale and proceed to exploit these with increasing levels of autonomy.

Case example – Claude – Agentic AI

Anthropic identified state actors using Claude, an agentic AI tool to systematically target Vietnamese critical infrastructure.

The state actor used Claude to enhance reconnaissance and attack capabilities.

This compromised major Vietnamese telecommunications providers, government databases, and agricultural management systems.

This took place over a 9-month campaign and was only identified through ad hoc threat hunting[5].

For information on mitigations for material risks see **3.3.2** of this chapter.

[5] Alex Moix, Ken Lebedev, Jacob Klein, **Threat Intelligence Report: August 2025**, Anthropic, 2025.

3.3 Best practice for identifying and mitigating risks

This section provides guidance on best practice mitigations for risks associated with cyber and information security hazards. Responsible entities should consider whether these mitigations will assist them in meeting their obligation to establish and maintain a process in their CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate any material risk of a cyber and information security hazard occurring and mitigate against relevant impacts (section 8(2) of the CIRMP Rules). The guidance does not comprehensively cover all possible mitigation or risks. The responsible entity must consider additional mitigations as required to address all potential material risks to the CI asset.

3.3.1 Material risks for consideration

Responsible entities must mitigate against the specified material risks in the CIRMP Rules, however they should also consider other possible material risks

Below are some suggested material risks for consideration. There may be other material risks that are not included in this guidance. It is the responsibility of the responsible entity to identify, eliminate, and minimise these material risks.

Risk Category	Description
Ransomware/Malware	Malicious software, including ransomware, can compromise systems and restrict access to critical data or operational technology. This may result in encryption of systems, disruption to business operations, or loss of availability of essential services. In some cases, malware may enable unauthorised access, lateral movement within the environment, exfiltration of sensitive data, or persistence mechanisms that allow continued exploitation of the CI asset. Supply chain mapping, as detailed in 7.4 of Chapter 7 – Supply chain hazards can assist in identifying this risk and is mandatory for responsible entities subject to the enhanced CIRMP. Mitigations such as patching (see **3.3.2.1**), phishing resistant MFA (see Chapter 4 – **Credential compromise hazards**), and network segregation (see Chapter 5 – **Lateral movement hazards**) can assist in mitigating this risk.
Internet-exposed services / misconfiguration	Internet-facing systems that are not securely configured can introduce vulnerabilities that may be exploited by malicious actors. Risks may arise from misconfigured services, open ports, or weak authentication controls. These exposures can allow unauthorised access, enable initial compromise of networks, support privilege escalation, or allow prepositioning for future attacks and disruption of the CI asset. Mitigations such as patching (see **3.3.2.1**), phishing resistant MFA (see Chapter 4 – **Credential compromise hazards**), and network segregation (see Chapter 5 – **Lateral movement hazards**) can assist in mitigating this risk.

3.3.2 Treating risk – mitigations and controls

3.3.2.1 Patching and updating in critical infrastructure environments

Patching and updating software, hardware, or other critical components in a timely manner can protect CI assets from known vulnerabilities. Responsible entities subject to the enhanced CIRMP are required to establish and maintain a process in their CIRMP to minimise or eliminate the material risk of failing to patch or update operating or security systems in a timely manner. However, it is best practice for all responsible entities to consider this risk when establishing their CIRMP.

What is a timely manner?

It is up to the responsible entity to determine an appropriate patching cadence. Responsible entities may wish to consider the suggestions below, noting it is not an exhaustive list.

- Establish a system or process in place to **receive and check advisories** on vulnerabilities from vendors of hardware and software as well from reputable agencies. Subscribe to relevant mailing lists (such as the **ASD's Alerts and Advisories**[6]) and read advisories promptly to check if any alerts are applicable to the technology environment(s).
- Consider **enabling automatic update features for patches** to hardware and software. There may be situations where this is not feasible or desirable and patches need to be applied manually after extensive testing. This is discussed in the next section.
- **Document patch governance processes**. Patching should be a systematic, coordinated and regularly applied process.
- **Prioritise patching based on the seriousness** of vulnerabilities, ease of exploitation and the specific level of risk to the organisation. For example, consider if the vulnerability relates to critical software or hardware – such as operating systems, security systems and/or internet facing systems. These may present a more immediate risk than unpatched systems in air-gapped networks or systems or software which are ancillary in nature.
- **Conduct regular vulnerability scans of systems**. The frequency of scans for different parts of the CI asset's environment should be adjusted based on level of risk and type of device (for example, internet-facing systems, internal workstations or servers, OT devices and network hardware may all have different frequencies). Cyber frameworks such as the ASD *Essential Eight* provide guidance on recommended frequencies for scans, although the timeframe should ultimately depend on the risk profile of the CI asset.

Challenges with patching in critical infrastructure environments

Timely patching for key systems and applications can be challenging in certain environments, such as where OT or other systems and devices have stringent uptime requirements for continuity of critical services and functions. In these environments, patches may only be able to be manually applied after in-depth consultation with device vendors and rigorous testing cycles to meet support and operational requirements. This may mean they cannot be applied in timeframes that would ordinarily be considered good practice, or as recommended by a particular cyber security framework.

If the responsible entity needs to implement compensating controls due to challenges in implementing timely patching, these controls and the reasons for their implementation should be documented in the CIRMP.

Examples of compensating controls could include:

- Robust network segmentation and the use of strict allow-listing via a secured gateway device to carefully limit connections to unpatched systems and devices until patches can be implemented.
- Ensuring that devices accessing critical systems, networks, devices or software are subject to real-time security posture checks.
- Restricting the availability and usage of administrative access privileges to unpatched systems and devices.
- Enhanced logging and monitoring of connections and network traffic to and from unpatched systems and devices to help rapidly identify and respond to suspicious activity.

[6] https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories

3.3.2.2 Managing the use of legacy systems and unsupported or obsolete hardware, software or critical components

Organisations may make use of legacy systems and unsupported or obsolete hardware, software or critical components (legacy technology) for operational reasons or due to other constraints. If the organisation cannot reasonably replace or update the system, then other measures should be put in place to address the risk.

Responsible entities subject to the enhanced CIRMP are required to establish and maintain a process in their CIRMP to minimise or eliminate the material risk of failing to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued. However, it is best practice for all responsible entities to consider this risk when establishing their CIRMP. Responsible entities may consider:

- Implementing transition plans that identify legacy technology and includes strategies, options and timeframes to migrate to more secure alternatives.
- Identifying and implementing compensating controls to limit security risks in the interim while transition plans are being executed. Examples include:
    - Using boundary or gateway services to allow for the implementation of modern security mechanisms (for example, MFA, device posture checks, and session logging and monitoring).
    - Limiting any connections between external networks and legacy technology. Ideally, these connections should occur via one or more hardened jump-hosts, with at least one placed in a separate network segment such as a de-militarised zone.
    - Ensuring that connections to and from legacy systems and external systems or services are restricted to just-in-time access wherever possible, thereby reducing the window of opportunity for attackers.
    - Using VLANs, firewalls and access control lists to isolate legacy, obsolete or unsupported parts of the environment from other systems, devices and assets.

When implementing other measures to address the risk of legacy technology responsible entities should consider triaging the technology to determine which ones are highest risk and prioritise applying mitigations to those systems or technologies. Responsible entities may consider these technologies higher risk due to their access to or storage of business critical data or the potential impact they may have on the availability, integrity, reliability or confidentiality of the CI asset.

3.3.2.3 Managing risks associated with novel, advanced and emerging technologies

Advanced, novel and emerging technologies include hardware, software, systems or processes that are newly developed or rapidly evolving. Examples include artificial intelligence, quantum computing, blockchain and advanced robotics.

As these technologies mature and become more accessible, the cyber threat landscape will evolve rapidly and develop greater proficiency to exploit existing vulnerabilities. These developments are not unexpected and strong cyber hygiene is the best defence.

The nature of these technologies means there may be new challenges and issues relating to maturity, security, reliability, and supply chain dependencies which may not be widely understood.

Responsible entities subject to the enhanced CIRMP must establish and maintain a process in their CIRMP to minimise or eliminate the material risk of:

- Deployment or hosting of advanced, novel or emerging technology; and
- Use of advanced, novel or emerging technology against the asset, in a manner that could prejudice the availability, integrity, reliability or confidentiality of the asset.

However, it is best practice for all responsible entities to consider this risk when establishing their CIRMP.

To effectively manage the deployment and use of these technologies, the responsible entity could adopt the following strategies:

Documentation	Clearly document risks associated with the technology that are specific to the CI asset, along with planned treatments for those risks. Risks and treatments should be reviewed regularly, reflecting the pace at which these technologies evolve. Relevant risk domains may include reliability, supply chain dependencies, attack paths, and integration challenges. Where appropriate, pilot testing or limited deployments can be used to assess risks prior to implementation in live operational environments.
Incident response and redundancy	Ensure incident response and redundancy plans are in place to address potential failures arising from the use of these technologies. This should include consideration of fallback or reversion to more conventional technologies while incidents are investigated and resolved.
Monitoring	Monitor reputable intelligence sources for information on emerging threats or attack vectors that leverage novel, advanced or emerging technologies. This includes consideration of how threat actors may use such technologies against the asset, even where the responsible entity does not intend to deploy them.

Example – Deployment of Artificial Intelligence with the CI asset

Many responsible entities are considering deploying AI into CI assets that could enhance the speed, quality and reliability of operational decisions. However, there are potential risks that should also be considered.

Reliability and traceability of decision

AI models can make decisions quickly with little transparency on the rationale for those decisions. They can also involve systematic bias that may only emerge from regular monitoring of specific decisions over a longer time period. Developers of AI may not understand the nuances of an entity's specific operational environments and could design their products to make decisions in a way which may not be suited to a particular CI asset. Should errors in decisions occur, it can lead to safety or operational issues that are difficult to troubleshoot.

Traceability of decision-making processes may also be important for safety and regulatory compliance. Ensuring AI outputs include transparent and clear explanations of decision-making processes is important so those decisions can be understood and validated. In addition, it will often be prudent to ensure vital decision points include a human in the decision-loop and that provisions are in place to ensure AI features can be easily disabled and reversion to manual operations can occur smoothly.

Overreliance on AI by operational workers

Over time, increasing reliance on AI within CI assets can lead to workforce de skilling. This may reduce personnel's ability to independently validate AI driven decisions and to safely operate systems manually, particularly during AI failures, system outages, or recovery scenarios. Maintaining manual operational capability through ongoing training and ensuring staff retain the skills necessary to assess and challenge AI based outcomes is therefore essential. Ensuring human accountability can also assist in ensuring personnel are incentivised to maintain appropriate oversight of critical decisions. Systems design is also key to ensure there is not undue pressure or influence on operators to defer to AI decisions.

Integration challenges

Integrating AI systems into OT environments can create complexities, particularly where an entity has legacy systems that are still in use. This may create interoperability challenges that could affect reliability of operations and make troubleshooting and recovery processes more complex. Organisations should ensure that any integration of AI is subject to thorough testing and evaluation and that plans are developed to transition away from legacy systems.

New attack surfaces

Integration of AI into OT environments can potentially result in new attack surfaces that malicious actors can target, particularly where external connectivity is required. This is in addition to new attack methods through the use of AI. Careful planning to identify potential vulnerabilities and attack paths should be undertaken to minimise the risk of exploitation and ensure response plans are in place.

Organisations are encouraged to patch as often as possible, particularly for software, hardware and services exposed to the internet, and use technologies to identify vulnerabilities and implement layered security.

Supply chain considerations

Processes for procuring AI products should be undertaken with careful consideration. This includes having a clear understanding of the provenance of any AI systems, models or components that an entity is considering acquiring. Responsible entities may require mandatory disclosure of training data and methods, risk assessments, safeguards and mitigations, and known incidents as part of their procurement due diligence.

Responsible entities should ensure that any data used for training AI models is under their control and not stored, handled or in any way modifiable by vendors or third parties without the entity's knowledge. Many AI products also integrate models from other providers, creating additional dependencies and potential vulnerabilities. It also important to understand the regulatory requirements that may apply to AI providers, particularly those in overseas jurisdictions. These may affect the safety and security of operations, data disclosure obligations, and increase the potential for geopolitical interference in the accessibility of their service.

Responsible entities should consider FOCI risks when implementing AI and other advanced and emerging technologies. For more information on this see provided at **2.2.4.2** of Chapter 2 – **All hazards**.

Example – Deployment of Artificial Intelligence against the CI asset

Advanced and emerging technologies can be used against CI assets and create or exploit new or unknown vulnerabilities in critical systems. An example of this is the deployment of AI against the CI asset.

Automation and scale of attacks

AI can enable malicious actors to automate reconnaissance and exploit vulnerabilities faster than traditional methods. AI tools can scan networks for weakness, identify misconfigurations or generate tailored attack methods with limited human intervention. This increase in speed and automation allows less sophisticated threat actors to exploit network vulnerabilities, where traditionally it required a level of expertise to do so.

This may result in more frequent attacks that are harder to detect or defend against.

Deception and manipulation through AI

AI can be used to generate more convincing phishing emails and voice impersonations as well as falsify data. AI can generate convincing phishing emails at far greater scale and with more accuracy and believability than human actors. This may increase a CI asset's vulnerability to this type of attack.

Frontier AI models

Frontier AI models are a rapidly developing threat. Frontier AI models are becoming more adept with each new generation, demonstrating a significant proficiency in reading, reasoning about and manipulating code. Frontier AI models are swiftly identifying existing vulnerabilities in software and are able to take advantage of these vulnerabilities at a greater rate than originally possible. To read more about this see the Australian Signals Directorate's Australian Cyber Security Centre's website[7].

3.3.2.4 Cyber threat intelligence sharing

Responsible entities that participate in cyber threat intelligence (CTI) sharing arrangements are better positioned to identify and respond to emerging cyber threats, including supply chain compromises, before they manifest within their own environment.

Participation in a peer CTI sharing arrangements is a voluntary risk management control that can support a responsible entity in meeting its duty to minimise or eliminate material risks of a cyber hazard and to mitigate the relevant impact of a hazard on the CI asset (section 8(2) of the CIRMP Rules).

Relationship to existing sharing and reporting obligations

Responsible entities should be aware that several distinct mechanisms exist for sharing and reporting cyber information.

These mechanisms operate at different layers – **strategic**, **operational**, and **technical/tactical** – and are complementary rather than substitutes for one another. The table below summarises these mechanisms.

[7] https://www.cyber.gov.au/about-us/view-all-content/news/frontier-models-and-their-impact-on-cyber-security-update

Intelligence sharing layers — definitions		
Layer	**What it covers**	**Typical content**
Strategic	High-level threat themes, policy dialogue, and sector-wide resilience priorities. Informs investment decisions and regulatory direction. Does not include specific technical indicators.	• Broadly observed threat themes (such as an increase in credential phishing). • Emerging trends of threat actors targeting specific sectors. • Policy and regulatory developments affecting the threat environment. • Sector-wide resilience gaps and investment priorities.
Operational	Tactics, techniques, and procedures (TTPs) used in attacks or incidents. Enables defenders to understand how threats operate and adjust controls accordingly.	• TTPs relating to attacks and incidents. • Security controls known to have been bypassed. • Threat actors being actively tracked. • Attack patterns observed across a sector.
Technical / Tactical	Specific technical indicators from incidents and blocked threats. The most operationally immediate layer — enables direct detection and blocking in security tooling.	• Technical indicators of compromise (IOCs) from incidents and blocked threats. • Indicators from active or emerging industry incidents (with permission). • Open-source technical indicators. • Common vulnerabilities exposures (CVE) advisories with exploitation context.

ASD's Cyber Threat Intelligence Sharing (CTIS) platform

The ACSC operates the CTIS platform to distribute threat information, including indicators of compromise, alerts, and advisories, to participating organisations. CTIS provides valuable government-sourced intelligence at the **technical/tactical layer** and participation is encouraged.

A well-resourced peer CTI sharing body can assist in translating, processing and contextualising CTIS output and redistributing actionable, prioritised intelligence to members in formats suited to their operational environment.

For more information, please see **Join the Cyber Threat Intelligence Sharing service through Sentinel or Splunk Enterprise Security | Cyber.gov.au**[8]

Benefits of peer CTI sharing

Peer CTI sharing can assist responsible entities to:

- identify supply chain compromises early
- calibrate material risk assessments
- reduce dwell time and incident impact
- operationalise government intelligence
- produce evidence of reasonable steps.

What to look for in a peer CTI sharing arrangement

Not all CTI sharing arrangements provide equivalent value. Responsible entities should assess prospective arrangements against both the quality of intelligence provided and the depth of technical infrastructure underpinning it. Some criteria to consider are:

- actionable intelligence relevant to the Australian threat environment
- cross-sector visibility
- translation and contextualisation of government intelligence
- compatibility with existing security operations

[8] https://www.cyber.gov.au/about-us/view-all-content/news-and-media/join-the-cyber-threat-intelligence-sharing-service-through-sentinel

- CVE monitoring and vulnerability intelligence infrastructure
- CVE Numbering Authority (CNA) status
- Software Bill of Materials (SBOM) analytical capability
- attack surface monitoring
- leaked credential monitoring
- trusted membership and governance.

Responsible entities should assess prospective sharing arrangements against these criteria and document their assessment as part of their CIRMP.

Relationship to supply chain obligations

Peer CTI sharing complements, but does not replace the supply chain mapping and vendor risk assessment obligations.

Where intelligence indicates a supplier has been compromised, responsible entities should have processes to assess exposure and activate relevant mitigations.

Responsible entities should consider whether their CIRMP includes a process for receiving, assessing, and acting on CTI relevant to their supply chain dependencies



3.4 Worked example – CIRMP Entry

Field	Example Response
Hazard	Failure or misuse of an artificial intelligence (AI) enabled decision support capability.
Asset(s) / Site	Primary Operations Centre – Site A. An AI-enabled Operations Decision Support Tool (ODST) is used by operational and technical support staff to analyse operational information and support time-critical decisions. The tool provides recommendations but does not take automatic operational action.
Scenario	An AI-enabled decision support tool provides incorrect recommendations, becomes unavailable during operations, or is misused following a cyber compromise. This affects the ability of staff to make timely and informed operational decisions.
Why this is material	The system supports important operational decisions and provides visibility over operational information. Errors, outages or misuse may disrupt operations, delay restoration or expose sensitive operational information.
Relevant impact mapping	**Availability:** disruption to operational decision-making and service delivery. **Integrity:** incorrect or manipulated recommendations may affect operational decisions and actions. **Confidentiality:** unauthorised access to sensitive operational information.
Evidence supporting likelihood	• ODST dependency mapping identifying the teams, systems and operational scenarios that rely on the tool. • Testing and performance records for recommendations, including identified errors and occasions where staff overrode the tool. • Vendor assurance material covering model updates, access, hosting, data handling and support arrangements.
Key dependencies / interdependencies *(Include here the cascading impact that may result from the realisation of the hazards)*	• Reliable operational data feeds and integrations used to generate recommendations. • Identity, authentication and remote-access services used by operational staff and vendor support personnel. • Operational staff who validate recommendations and maintain situational awareness. • Incorrect outputs or loss of the tool could delay decisions and create cascading impacts across dependent operational functions.
Controls — Preparedness	• Maintain incident playbooks for incorrect recommendations, suspected manipulation, tool outage, credential compromise and vendor incidents. • Maintain documented decision checks and manual operating procedures.
Controls — Prevent / minimise likelihood	• Operate ODST in advisory mode, with no automatic operational actions, until reliability and assurance requirements are met. • Monitor for unusual access, unexpected recommendation patterns and changes in system behaviour. • Apply strong authentication, least privilege and controlled remote access for operational and vendor accounts.
Controls — Impact mitigation	• Require staff to validate AI recommendations against documented checks before acting. • Maintain a clear process to disable ODST and switch to manual procedures. • Revoke affected access, isolate compromised systems and preserve relevant logs following suspected misuse.
Owners / status / timeframes	• ODST integration and configuration control — Operations Systems Manager (In progress; Dec 2026). • Identity, access and monitoring controls — Cyber Security Lead (Implemented; quarterly review). • Operational decision checks and manual procedures — Operations Manager, Site A (Implemented; next exercise Nov 2026).

Residual risk and acceptance	Residual risk assessed as medium due to evolving AI-related threats, dependence on vendor support and data feeds, and the potential for plausible but incorrect recommendations. Accepted by the Risk Committee (May 2026), subject to completion of system separation and vendor assurance actions and continued human validation of recommendations.
Review cadence / triggers	Review annually as part of the CIRMP cycle and quarterly during rollout. Trigger review after: • a significant ODST, model, data-source or integration update • a change to the vendor, hosting location, support model or access arrangements • an incorrect recommendation, outage, cyber incident or near miss • evidence of unusual access, manipulation or unexpected system behaviour
Supporting material	• ODST architecture, dependency and data-flow documentation • Documented operational decision checks and manual procedures • Exercise plans, after-action reports and improvement actions • Monitoring rules, incident playbooks and escalation contacts

Table of contents: Chapter 4

4.1 Obligations for managing a credential compromise hazard 56
4.2 Meeting the obligations in practice 57
4.2.1 Outline the systems or networks where phishing resistant (MFA) is required to authenticate 57
4.2.2 Minimise or eliminate a material risk, and mitigate the relevant impact 57
4.2.3 Implement phishing resistant MFA 58
4.2.4 Centrally log, monitor, and review MFA attempts 59
4.3 Best practice for identifying and mitigating risks 59
4.4 Worked example – CIRMP entry 59

4. Credential compromise hazards

The compromise or misuse of credentials presents a persistent and significant risk, enabling malicious actors to gain unauthorised access to critical components, including critical systems.

The compromise of credentials is often an entry point for broader cyber incidents. Malicious actors may gain access to a system through unauthorised use of credentials and then introduce vulnerabilities into the system. This may affect the availability, integrity, reliability or confidentiality of a CI asset. The consequences of credential compromise may include unauthorised access to systems or business critical data, pre-positioning within systems for future malicious activity, and disruption to operations or degradation of asset functionality.

Effectively managing credential compromise hazards is essential to maintaining the security, integrity and resilience of CI assets.



4.1 Obligations for managing a credential compromise hazard

The table below outlines the obligations in the CIRMP Rules in relation to credential compromise hazards. It outlines whether the obligations apply to responsible entities subject to the baseline and/or enhanced CIRMP requirements and/or TSRMP requirements. The obligations are expanded on later in this chapter.

It should be noted that the below information only applies to responsible entities who are complying with a cyber security framework that **does not** require the implementation of phishing resistant MFA controls (section 8B(1) of the CIRMP Rules).

Credential compromise hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Responsible entities must establish and maintain a process or system in their CIRMP to — so far as is reasonably practicable to do so — outline the systems or networks where phishing resistant multi-factor authentication (MFA) is required to authenticate: (i) access to their organisation's internet connected computers and critical systems; (ii) privileged and unprivileged access to critical components; (iii) remote access to computer applications, systems or services.		s 8B(3)(a)	
Responsible entities must establish and maintain a process or systemin their CIRMP to — so far as it is reasonably practicable to do so — to: (b) minimise or eliminate any material risk of a credential compromise hazard occurring; and (c) mitigate the relevant impact of the credential compromise hazard on the CI asset.		s 8B(3)(b) s 8B(3)(c)	
If a responsible entity implements the MFA controls in section 8B(5)(a) and section 8B(5)(b) they are taken to have acquitted the obligation to minimise or eliminate any material risk that a credential compromise hazard could have a relevant impact on the asset. The MFA controls in sections 8B(5)(a) and (b) are as follows: a) implement phishing resistant MFA controls for the systems and networks outlined in s 8B(3)(a); and b) centrally log, monitor and routinely review both successful and unsuccessful MFA attempts.		s 8B(4) s 8B(5)	

Timeframes for compliance are explained in Chapter 1 – **Introduction to the critical infrastructure risk management program (CIRMP)** at **1.5**

4.2 Meeting the obligations in practice

4.2.1 Outline the systems or networks where phishing resistant (MFA) is required to authenticate

Best practice for all responsible entities to consider

CIRMP enhanced - section 8B(3)(a)

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain a process or system in their CIRMP to – so far as is reasonably practicable – outline the systems or networks where phishing resistant MFA is required to authenticate.

- Access to the organisation's internet connected computers and critical systems.
- Privileged and unprivileged access to critical components.
- Remote access to computer applications, systems or services.

Systems that are internet-facing, enable remote access, or provide access to critical systems and critical components are at heightened risk. Identifying these systems allows responsible entities to prioritise the implementation of phishing resistant MFA where compromise would introduce a material risk to the CI asset.

In practice, responsible entities should undertake a structured assessment of their environment to determine where MFA is required. This may include:

- Identifying all internet-connected systems and services.
- Mapping remote access pathways, including third-party and vendor access.
- Identifying critical components and critical systems.
- Assessing the potential impact of credential compromise for each system.

This process should be ongoing and regularly reviewed to ensure that changes to systems, IT or OT environments, or threat environment are captured.

4.2.2 Minimise or eliminate a material risk, and mitigate the relevant impact

Best practice for all responsible entities to consider

CIRMP enhanced - section 8B(3)(b) & (c)

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain processes or systems to – so far as it is reasonably practicable to do so – minimise or eliminate any material risk of a credential compromise hazard occurring and mitigate the relevant impact of such a hazard on the CI asset.

Responsible entities should ensure that identified risks are documented, regularly reviewed, and supported by appropriate mitigations proportionate to the level of risk.

By implementing the phishing resistant MFA controls set out in section 8B(5), responsible entities can acquit the obligation to minimise or eliminate any material risk of a credential compromise hazard. Broadly, the phishing resistant MFA controls in section 8B(5) require a responsible entity to:

- authenticate access to certain systems and networks (see **4.2.3** of this chapter); and
- centrally log, monitor and routinely review both successful and unsuccessful MFA attempts (see **4.2.4** of this chapter).

If a responsible entity cannot implement the MFA controls in section 8B(5), they should still include a process or system in their CIRMP containing reasonable steps that must be taken to minimise or eliminate the material risks associated with the occurrence of a credential compromise hazard, in line with the general obligation in section 8B(3).

4.2.3 Implement phishing resistant MFA

Best practice for all responsible entities to consider

CIRMP enhanced – sections 8B(4) and (5)(a)

Under section 8B(5), the first requirement for phishing resistant MFA controls is that they are implemented to authenticate:

- access to their organisation's online and internet-facing networks
- privileged and unprivileged access to critical components
- remote access to their computer applications, systems or services.

Phishing resistant MFA provides a second line of defence against credential stuffing, phishing, adversary-in-the-middle/relay attacks and other types of cyber attacks involving compromised account credentials. Its use in critical infrastructure environments is vital for managing access to critical systems and internet-facing networks (including remote access scenarios).

There may be alternative measures the responsible entity needs to take where it is not feasible to implement phishing resistant MFA. Where a responsible entity cannot implement phishing resistant MFA , they must include a process in their CIRMP containing reasonable steps that must be taken to minimise or eliminate risks associated with the occurrence of a credential compromise hazard in line with the general obligation in section 8B(3).

Challenges with using MFA in critical infrastructure

Implementation of phishing resistant MFA can be challenging in certain environments. The nature of a system or technology may prevent the use of MFA (such as legacy systems), or the operational environment or context of the CI asset may result in MFA being impractical.

For example, real-time operational and safety constraints may mean that staff (such as field technicians and engineers) need to respond to alerts from devices in an extremely short timeframe, particularly in emergency situations. The use of MFA workflows in these scenarios may be difficult without creating safety issues or interfering with the execution of key processes.

Similarly, OT networks may be air-gapped or otherwise isolated from other networks either intermittently or for an extended period, which can make the use of cloud-based MFA mechanisms impractical.

In these scenarios, the organisation should consider using additional controls to compensate for the absence of phishing resistant MFA where necessary. Examples include:

- Ensuring only managed, hardened endpoints (such as devices supplied and pre-configured securely by the organisation) can access legacy components or obsolete technology.
- Ensuring passwords are of an adequate length and are unique, to assist in mitigating against brute force and credential stuffing attacks.
- Using hardware based one-time password tokens or application-based codes;
- Using jump-hosts or similar boundary services.
- Prohibiting the use of shared accounts for access to critical networks and systems.
- Strictly enforcing principles of least-privilege and time-bound access for important operational or administrative tasks.
- Considering using of out-of-band approval processes or dual-control workflows for any critical activities such as major configuration changes or key operational actions.

Note that this is not an exhaustive list and there may be other measures that are appropriate to implement in addition to or in lieu of the above.

If the use of any form of phishing resistant MFA is not possible, it would be expected that the reasons for this are clearly articulated in the CIRMP and that alternative controls are implemented.

4.2.4 Centrally log, monitor, and review MFA attempts

Best practice for all responsible entities to consider

CIRMP enhanced - section 8B(5)(b)

The second requirement in section 8B(5) for phishing resistant MFA controls is that responsible entities centrally log, monitor and routinely review both successful and unsuccessful MFA attempts.

Logs can help identify suspicious login patterns that can indicate a potential breach. These may include:

- Repeated failed attempts to access critical systems from other networks.
- Attempted access to critical systems occurring at unusual times.
- Access attempts to critical system from unauthorised devices or networks.

Logging these attempts provides the responsible entity with valuable information, and the ability to detect anomalies and potential risks. This information should be stored in a secure location where the content cannot be altered by unauthorised users. If a malicious actor is operating in the CI asset's system and the records of MFA attempts are easily altered, the malicious actor may be able to conceal their actions. As such, it is essential that this information is stored securely.

While it is a matter for responsible entities to establish a routine review cycle, ideally logs should be reviewed daily through an automatic process to ensure any attempted or actual breaches are identified quickly. This can be supplemented with manual reviews on a less-frequent basis (such as weekly) to help identify any ongoing trends or patterns. Consider reviewing for suspicious login patterns on at least a weekly basis, with more regular reviews (such as daily) for high-risk accounts such as those with administrative privileges.

4.3 Best practice for identifying and mitigating risks

For responsible entities subject to the baseline CIRMP or TSRMP, it is best practice to address credential compromise hazards through the controls outlined at **4.2.3** and **4.2.4**.

4.4 Worked example – CIRMP entry

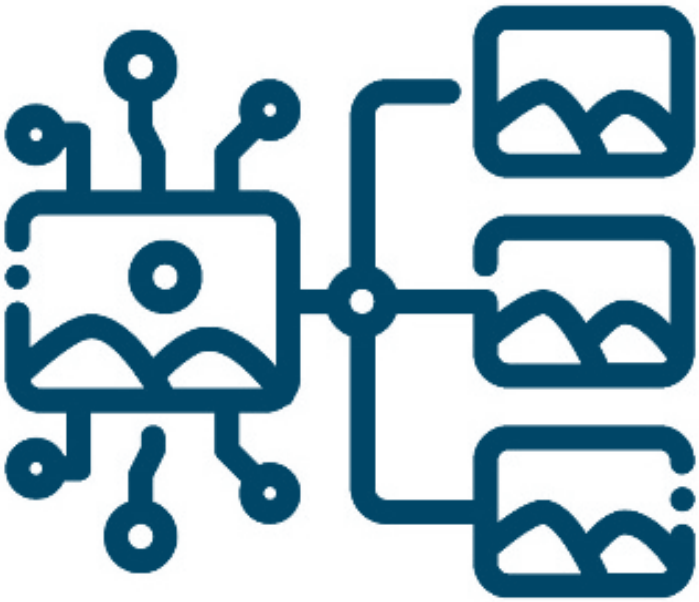
Field	Example Response
Hazard	Compromise and misuse of credentials used to access internet-connected systems and remote access services.
Asset(s) / Site	Corporate network and remote access gateway supporting access to critical systems used to monitor and manage essential services.
Scenario	Credentials used to authenticate remote access to systems are obtained by a malicious actor through a phishing attack. The actor uses the compromised credentials to gain unauthorised access to internet-connected systems and critical components via remote access pathways.
Why this is material	• Unauthorised access using valid credentials may allow malicious activity to appear legitimate and avoid detection. • Access via remote authentication pathways may enable interaction with critical systems and components, increasing the risk of disruption or manipulation of services.
Relevant impact mapping	Availability: disruption or degradation of services due to unauthorised system actions. Integrity: unauthorised changes to configurations, processes, or operational data. Confidentiality: unauthorised access to sensitive operational or system information.

Evidence supporting likelihood	• Industry reporting identifying credential-based attacks (phishing and credential reuse) as a common initial access vector. • Logs indicating repeated failed authentication attempts across remote access services. • Prior security assessments identifying gaps in authentication controls or credential management practices.
Key dependencies / interdependencies (Include here the cascading impact that may result from the realisation of the risk)	Dependent on secure authentication and access control across: • Remote access services and gateways. • Identity and authentication systems. • Systems supporting monitoring and management of critical components. • Internet-connected services and infrastructure.
Controls — Preparedness	• Implementation of authentication controls (including phishing resistant MFA) for remote and internet-facing access. • Processes for identifying systems requiring strong authentication controls. • Playbooks for responding to credential compromise (credential reset, investigation).
Controls — Prevent / minimise likelihood	• Limiting access permissions associated with credentials (least privilege). • Secure management of credentials, including storage, rotation, and revocation.
Controls — Impact mitigation	• Rapid revocation and reset of compromised credentials. • Monitoring and detection of anomalous authentication activity. • Isolation of affected systems or accounts where unauthorised access is identified.
Owners / status / timeframes	Authentication controls implementation — Security Lead — In progress; Dec 2026. Monitoring and logging improvements — Security Operations Lead — Planned; Oct 2026.
Residual risk and acceptance	Residual risk assessed as medium due to ongoing exposure to credential-based attacks targeting internet-facing systems. Risk accepted by Risk Committee (Jun 2026).
Review cadence / triggers	Formal review annually as part of CIRMP review. Trigger review after: • any suspected or confirmed credential compromise event • significant changes to authentication systems or remote access architecture • changes in threat level due to imminent or actual crisis/conflict.
Supporting material	• Authentication and access control policies • Authentication logs and monitoring reports • Credential lifecycle management procedures



Table of contents: Chapter 5

5.1 Obligations for managing lateral movement hazards 62
5.2 Meeting the obligations in practice 63
5.2.1 Identify and maintain an inventory of critical systems 63
5.2.2 Recovery, restoration and maintaining availability 63
5.2.3 Continued availability while rebuilding or restoring critical systems 64
5.2.4 Minimise or eliminate material risks and mitigate relevant impacts 64
5.2.5 Implement network segregation 65
5.2.5.1 Implementing network segregation in practice 65
5.2.5.2 Logical access controls 66
5.2.5.3 Logging, monitoring, and reviewing access logs 66
5.2.5.4 Implementation of least privilege across networks 66
5.3 Best practice for identifying and mitigating risks 66
5.4 Worked example – CIRMP entry 67



5. Lateral movement hazards

Lateral movement hazards relate to the risk of unauthorised activity spreading across systems and networks within a CI asset after an initial point of access has been established. This may occur where a malicious actor or unauthorised agent moves between critical systems or connected computers to expand access, escalate privileges, or disrupt operations.

Lateral movement hazards are particularly relevant in environments where systems are interconnected or share trust relationships. If not effectively managed, these hazards may allow a localised compromise to propagate across systems, increasing the scale and impact of an incident. They may also enable an adversary to undertake prepositioning activities, whereby access is established or maintained across multiple systems in preparation for unauthorised actions. This may affect the availability, integrity, or reliability of the CI asset, or the confidentiality of information related to the CI asset.

5.1 Obligations for managing lateral movement hazards

The table below outlines the obligations in the CIRMP Rules in relation to lateral movement hazards. It outlines whether the obligations apply to responsible entities subject to the baseline and/or enhanced CIRMP requirements and/or TSRMP requirements. The obligations are expanded on later in this chapter.

Lateral movement hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Responsible entities must establish and maintain a process or system to identify and maintain an inventory of critical systems and how they are connected with other critical systems and other computers.		s 8C(2)(a)	
Responsible entities must establish and maintain a process or system to recover and restore critical systems in the event where an incident has had or is having a relevant impact on the asset.		s 8C(2)(b)	
Responsible entities must establish and maintain a process or system to ensure the continued availability of the asset whilst rebuilding or restoring critical systems.		s 8C(2)(c)	
Responsible entities must establish and maintain a process or system to – as far as reasonably practicable to do so: (i) minimise or eliminate any material risk of a lateral movement hazard occurring; and (ii) mitigate the relevant impact of the lateral movement hazard on the CI asset.		s 8C(2)(d)	
If a responsible entity implements the network segregation in section 8C(4) they are taken to have acquitted the obligation to minimise or eliminate the material risks that a lateral movement hazard could have a relevant impact on the CI asset. The network segregation in section 8C(4) are as follows: (a) ensuring critical systems can be segregated as between critical systems, and between critical systems and other computers; (b) ensuring critical systems can be operationally independent from other internet connected computers and critical systems; (c) ensuring critical systems can continue to be operational for a period of at least three months while other computers are in a state of restoration or recovery; (d) implementing logical access controls for network traffic between critical systems, and between critical systems and other computers;		s 8C(4)	

(e) centrally logging, monitoring and routinely reviewing access logs for communication paths between critical systems, and between critical systems and other computers; and (f) implementing principles of least privilege across computers that connect to critical systems.			

Timeframes for compliance are explained in Chapter 1 – **Introduction to the critical infrastructure risk management program (CIRMP)** at **1.5**

5.2 Meeting the obligations in practice

5.2.1 Identify and maintain an inventory of critical systems

Best practice for all responsible entities to consider

CIRMP enhanced - section 8C(2)(a)

Responsible entities for CI assets subject to the enhanced CIRMP must identify and maintain an inventory of critical systems and an understanding of how those systems are connected to other critical systems and computers.

Responsible entities should first identify all their systems (specifically IT and OT). Merely looking at what is believed to be critical may result in missing systems that are smaller, more discrete, or perceived as less important. Once this is complete, responsible entities can consider whether these systems are critical systems. Critical systems are important to the delivery of the function of the asset. For the definition of **critical systems** please see the **glossary**.

Responsible entities should also consider system interdependencies when identifying and documenting critical systems. Understanding how systems are connected is a key component of managing lateral movement hazards. Lateral movement relies on the ability to traverse systems through existing pathways or trust relationships. Identifying how critical systems, supporting systems, and internet-connected computers interact with each other allows responsible entities to understand where unauthorised movement between systems may occur.

This inventory should be regularly reviewed and updated to ensure currency.

5.2.2 Recovery, restoration and maintaining availability

Best practice for all responsible entities to consider

CIRMP enhanced - section 8C(2)(b)

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain processes or systems to recover and restore critical systems in the event an incident has had or is having a relevant impact on the entity..

Lateral movement hazards may result in the compromise or disruption of multiple interconnected systems. Where an incident spreads across systems, recovery activities may need to be undertaken across several parts of the environment simultaneously. The ability to restore systems in a controlled manner while maintaining the continued operation of the CI asset is critical to limiting the overall impact of such events.

In practice, responsible entities should establish processes that support the recovery and restoration of critical systems. These may include:

- Clear procedures for restoring systems following compromise or disruption.
- Defined sequencing of recovery activities, taking into account dependencies between systems.
- Contingency options, such as redundant systems or alternative operating arrangements, to support continuity of operations.

Responsible entities should ensure that critical systems can operate independently from other systems during restoration activities. This includes the ability for critical systems to remain operational where other systems are unavailable or undergoing recovery. Responsible entities should also ensure that recovery and restoration processes are designed to avoid introducing further risk to systems, including preventing the reintroduction or spread of compromise during system rebuild activities.

These processes should be proportionate to the level of risk and complexity of the CI asset environment and should be regularly tested and reviewed to ensure they remain effective.

5.2.3 Continued availability while rebuilding or restoring critical systems

Best practice for all responsible entities to consider

CIRMP enhanced - section 8C(2)(c)

Responsible entities with CI assets subject to the enhanced CIRMP must establish and maintain processes or systems to ensure the continued availability of the asset whilst rebuilding or restoring critical systems.

Network segregation, which is discussed further in **5.2.5**, contributes to the ability of responsible entities to quarantine impacted critical systems and ensure any breaches or degradation of a system cannot spread further. This segregation can prevent a breach from proliferating throughout systems and ensure continued availability of non-impacted systems.

To support ensuring continued availability while rebuilding or restoring critical systems, responsible entities may consider:

- Enabling systems to operate in offline or local modes where appropriate.
- Implementing local redundancy or failover mechanisms that do not rely on external systems.
- Maintaining access to critical system configurations, processes and procedures.
- Ensuring availability of required resources, including spare components, to support ongoing operations.
- Ensuring compromised systems are appropriately isolated to prevent the spread or reintroduction of compromise during recovery activities.
- Periodically running simulations of scenarios where critical systems need to run independently of other systems to verify the measures in place are appropriate.

Responsible entities should consider undertaking tabletop exercises and ensure they have appropriate incident response processes in place.

5.2.4 Minimise or eliminate material risks and mitigate relevant impacts

Best practice for all responsible entities to consider

CIRMP enhanced - section 8C(2)(d)

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain processes or systems to – so far as it is reasonably practicable to do so – minimise or eliminate any material risk of a lateral movement hazard occurring and mitigate the relevant impact of the hazard on the CI asset.

If a responsible entity who is subject to the enhanced CIRMP applies network segregation as listed in section **5.2.5** of this chapter, then they will be considered to have acquitted the obligation to minimise or eliminate the material risk of a lateral movement hazard having a relevant impact on the CI asset.

If a responsible entity cannot implement the network segregation set out in section 8C(4), they should still include a process or system in their CIRMP containing reasonable steps that must be taken to minimise or eliminate the material risks associated with the occurrence of a lateral movement hazard, in line with the general obligation in section 8B(3).

Responsible entities should ensure that identified risks are documented, regularly reviewed, and supported by appropriate mitigations proportionate to the level of risk.

5.2.5 Implement network segregation

Best practice for all responsible entities to consider

CIRMP enhanced - section 8C(4)

Responsible entities for CI assets subject to the enhanced CIRMP should implement the below elements to achieve network segregation of critical systems.

- Ensuring critical systems can be segregated as between critical systems, between critical systems and other computers.
- Ensuring critical systems can operate independently from other internet connected computers and critical systems.
- Ensuring critical systems can continue to be operational for a period of at least three months while other computers are in a state of restoration or recovery.
- Implementing logical access controls for network traffic between critical systems, and between critical systems and other computers.
- Centrally logging, monitoring and routinely reviewing access logs for communication paths between critical systems, and between critical systems and other computers.
- Implementing principles of least privilege across computers that connect to critical systems.

Network segregation is a key control for managing lateral movement hazards. It limits the potential for unauthorised activity to spread between systems by restricting communication pathways and ensuring that critical systems can operate independently from other systems.

Responsible entities subject to the baseline CIRMP should consider whether this mitigation is appropriate to implement depending on the material risks that apply to them.

5.2.5.1 Implementing network segregation in practice

Responsible entities should design their environments so that connectivity between systems is limited to what is operationally required. This involves separating critical systems from other systems and restricting how and when communication between those systems can occur.

In practice, this may involve structuring environments to:

- Separate critical systems from corporate IT environments and other networks to limit unnecessary interaction.
- Tightly control communication between systems and only permit it where required for the delivery of the asset's function.
- Clearly define and manage access pathways between systems, rather than leaving them broadly accessible.

Other approaches may be used to strengthen segregation, dependent on the environment. For example, responsible entities may apply highly granular separation of systems and services to ensure that communication between devices is strictly controlled. This can reduce the likelihood that an issue affecting one system can propagate across the environment. Similarly, administrative or management interfaces for critical systems may be isolated from general-purpose networks to reduce the risk of unauthorised access.

In some environments, achieving operational independence may also require physical separation of systems or supporting infrastructure. This should be assessed based on the risk profile and architecture of the asset.

Responsible entities should also consider how dependencies between systems may affect their ability to maintain segregation. Where systems rely on centralised services, enterprise platforms or external providers, those dependencies may introduce pathways for lateral movement or create challenges in maintaining operational independence. Minimising reliance on external or shared services, where appropriate, can assist in maintaining system integrity during an incident.

Connections to external networks should be carefully controlled and monitored. Environments that rely on multiple external connections or integrate with third-party systems may experience additional risks if those external systems are compromised. Managing these connections through controlled and centralised access points can reduce the number of potential pathways into and across the environment and improve visibility over system interactions.

5.2.5.2 Logical access controls

Responsible entities should implement logical access controls to restrict communication between critical systems and other networks. These controls determine which systems are permitted to communicate and under what conditions.

Logical access controls should ensure that communication between systems is limited to what is required for operational purposes. This may include restricting which systems can initiate connections, limiting the types of communication permitted, and ensuring that unnecessary pathways are removed.

Examples of logical access controls include the use of network segmentation technologies, access control mechanisms, and filtering tools that regulate how systems interact with one another.

5.2.5.3 Logging, monitoring, and reviewing access logs

Responsible entities should centrally log, monitor and routinely review communication between critical systems and other networks. This supports the identification of potential lateral movement and other anomalous behaviour within the environment.

In practice, responsible entities should maintain visibility over how systems interact and monitor for indicators such as:

- repeated failed attempts to access critical systems from other networks.
- attempted access to critical systems occurring at unusual time.
- unusual amounts of data transiting between networks containing critical systems and other network zones.
- access attempts to critical system from unauthorised devices or networks.

These logs provide valuable information for responsible entities in addressing potential threats and risks. This information significantly decreases in value if it is stored insecurely. Responsible entities should ensure that they are storing these logs in secure systems so they can ensure that the information is not altered in an attempt to disguise malicious activity.

While it is up to the responsible entity to determine what a routine review cycle looks like, ideally logs should be reviewed daily through an automatic process to ensure any attempted or actual breaches are identified quickly. This can be supplemented with manual reviews on a less-frequent basis (such as weekly) to help identify any ongoing trends or patterns. Responsible entities may also consider the use of real-time alerts.

5.2.5.4 Implementation of least privilege across networks

Responsible entities should implement the principle of least privilege across systems that connect to critical systems.

In the context of lateral movement hazards, this involves limiting the ability for systems, services and processes to access other systems to what is necessary. Restricting system-to-system access reduces the number of pathways available for unauthorised movement and limits the potential impact of a compromise.

Responsible entities should ensure that access between systems is appropriately restricted, regularly reviewed, and aligned to operational requirements. This includes limiting permissions, removing unnecessary access pathways, and maintaining appropriate oversight of system interactions. Further technical guidance on implementing network segregation and related controls can be found in the Australian Signals Directorate's **CI Fortify**[9].

5.3 Best practice for identifying and mitigating risks

For responsible entities subject to the baseline CIRMP or TSRMP, it is best practice to address lateral movement hazards through the controls outlined in **5.2.5**.

[9] https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/ci-fortify

5.4 Worked example – CIRMP entry

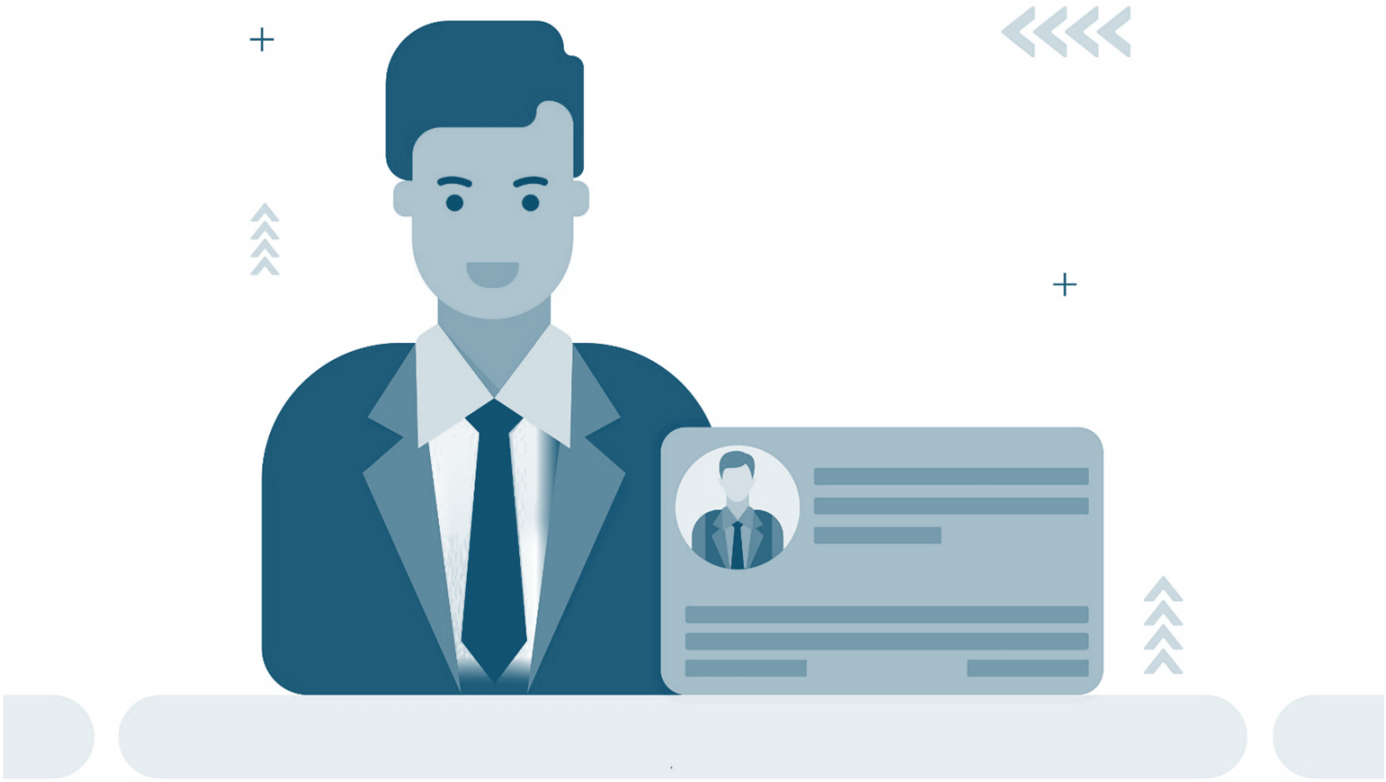
Field	Example Response
Hazard	Unauthorised movement between connected systems following an initial compromise, resulting in disruption across critical systems.
Asset(s) / Site	Operational network supporting control systems for essential service delivery. Includes multiple interconnected critical systems and supporting IT infrastructure.
Scenario	An attacker gains access to a non-critical system connected to the corporate IT environment. Due to inadequate segregation and unrestricted communication pathways, the attacker moves between systems and accesses connected critical systems. The attacker accesses multiple systems using existing trust relationships and communication pathways.
Why this is material	Lateral movement between systems may allow a compromise affecting one system to spread across multiple systems within the CI asset. Movement across systems may allow unauthorised activity to persist undetected and increase the scale and impact of an incident.
Relevant impact mapping	**Availability:** disruption to service delivery due to multiple systems being affected. **Integrity:** unauthorised modification of system configurations or operational processes. **Confidentiality:** unauthorised access to sensitive system or operational information. **Reliability:** degradation in system performance and reduced confidence in system outputs.
Evidence supporting likelihood	• Prior security reviews identifying limited segregation between IT and OT systems. • Observed system architectures with broad or unnecessary communication pathways. • Intelligence reports indicating prepositioning in critical infrastructure is a relevant risk.
Key dependencies / interdependencies (Include here the cascading impact that may result from the realisation of the risk)	Dependent on connectivity between: • critical systems supporting essential operations. • corporate IT networks and supporting systems. • shared services and infrastructure (authentication, monitoring or data services).
Controls — Preparedness	• Identification and mapping of system connections and dependencies. • Playbooks for responding to incidents involving multiple compromised systems.
Controls — Prevent / minimise likelihood	• Restricting communication pathways between systems to only what is operationally required. • Applying network segregation between critical systems and other environments. • Limiting system-to-system access through least privilege principles.
Controls — Impact mitigation	• Isolating affected systems to prevent further spread of compromise. • Monitoring system communication to detect anomalous behaviour. • Sequencing recovery of systems based on dependencies and criticality.
Owners / status / timeframes	• Network architecture review — Engineering Lead — In progress; Nov 2026. • Segregation controls uplift — Security Team — Planned; Jan 2027.
Residual risk and acceptance	Residual risk assessed as medium due to system complexity and interdependencies. Risk accepted by Risk Committee (Jun 2026).
Review cadence / triggers	Formal review at 24 months as part of CIRMP review. Trigger review after: • any incident involving system-to-system propagation. • significant changes to system architecture or connectivity. • identification of new interdependencies or access pathways.
Supporting material	• Network segmentation design documentation. • Monitoring and logging reports. • Incident response and recovery procedures.

Table of contents: Chapter 6

6.1 Obligations for managing personnel hazards 70
6.2 Meeting the obligations in practice 71
6.2.1 Identify the critical workers 71
6.2.2 Restrict access to critical workers assessed to be suitable 73
6.2.2.1 Identifying if a critical worker is suitable 74
6.2.3 Minimise or eliminate specified material risks 75
6.2.3.1 Risk arising from remote access to operational control or operational monitoring systems of the CI asset 75
6.2.3.2 Risk arising from off-boarding process for outgoing employees and contractors 76
6.2.4 Minimise or eliminate the material risks (enhanced) 76
6.2.4.1 Risk associated with unauthorised or unsupervised access to critical components 76
6.2.4.2 Risk associated with compromise or misuse of credentials and privileged access used by individuals to access the CI asset 77
6.2.4.3 Risk associated with access to the CI asset by persons other than critical workers for the CI asset 77
6.2.4.4 Risk arising from incoming or outgoing critical workers 78
6.2.5 Suitability assessment of critical workers that have access to critical components 78
6.2.5.1 Relevant security clearance 79
6.2.5.2 Risk assessment of critical worker unable to meet requirements 79
6.2.6 Monitor suitability of critical workers 80
6.3 Best practice for identifying and mitigating risks 81
6.3.1 Material risks for consideration 81
6.3.2 Treating risk – mitigations and controls 82
6.3.2.1 Managing adverse critical worker suitability findings 82
6.3.2.2 Establishing a positive security culture 83
6.3.2.3 Security awareness training 83
6.3.2.4 Knowledge transfer and record keeping procedures 84
6.3.2.5 Off-boarding processes 85
6.3.2.6 Insider threat monitoring 85
6.3.2.7 Clean desk policies 85
6.3.2.8 Visitor procedures 86
6.3.2.9 Overseas travel policies 86
6.4 Worked example – CIRMP entry 88

6. Personnel hazards

Personnel hazards are a significant factor in the security, resilience, and continuity of CI assets. Personnel hazards can arise from malicious external actors, trusted insiders, or unintentional actions such as human error or unsafe practices from internal workers. Personnel can deliberately or inadvertently compromise an asset through negligence, misuse of access, or malicious conduct. Conversely, personnel can play a role in protecting an asset. Having security minded, well-trained workers can assist in early identification of hazards or incidents and strengthen resilience. Effectively managing personnel hazards requires the responsible entity to recognise both the risks posed by personnel and the essential role they play in safeguarding CI assets.



6.1 Obligations for managing personnel hazards

The table below outlines the obligations in the CIRMP Rules in relation to personnel hazards. It outlines whether the obligations apply to responsible entities subject to the baseline and/or enhanced CIRMP requirements and/or TSRMP requirements. The obligations are expanded on later in this chapter.

Personnel hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Responsible entities must establish and maintain a process or system in the entity's CIRMP to identify the entity's critical workers.	s 9(1)(a)	s 9(1)(a)	s 12(1)(a)
Responsible entities must establish and maintain a process or system in the entity's CIRMP to permit a critical worker access to critical components of the CI asset only where the critical worker has been assessed to be suitable to have such access.	s 9(1)(b)	s 9(1)(b)	s 12(1)(b)
Responsible entities must establish and maintain a process or system in the entity's CIRMP, to – as far as it is reasonably practicable to do so – minimise or eliminate the material risks: (i) arising from malicious or negligent employees or contractors; and (ii) arising from the off-boarding processes for outgoing employees and contractors.	s 9(1)(c)	s 9(1)(c)	s 12(1)(c)
Responsible entities must establish and maintain a process or system in the entity's CIRMP to minimise or eliminate the material risks associated with: (a) unauthorised or unsupervised access to critical components; (b) the compromise or misuse of credentials and privileged access used by individuals to access the CI asset; (c) access to the CI asset by persons other than critical workers for the CI asset; and (d) incoming and outgoing critical workers.		s 9A (2)	
Responsible entities must establish and maintain a process or system in the entity's CIRMP to permit a critical worker access to critical components only where they have been assessed to be suitable (i) the critical worker has been assessed to be suitable in accordance with subsection 9A(4) [see information contained at 6.2.5]; or (ii) if the critical worker is unable to meet the requirements outlined in subsection 9A(4) – the responsible entity has outlined in their CIRMP the risk associated with the employment of the critical worker and actions taken, or action that will be taken as soon as reasonably practicable to do so, to minimize or eliminate the risk to the asset.		s 9A(3)(a)	
Responsible entities must establish and maintain a process or system in the entity's CIRMP to proactively monitor, identify and take action in relation to any developments or changes that may affect the ongoing suitability of a critical worker.		s 9A(3)(b)	

Timeframes for compliance are explained in Chapter 1 – **Introduction to the critical infrastructure risk management program (CIRMP)** at **1.5**

6.2 Meeting the obligations in practice

6.2.1 Identify the critical workers

CIRMP baseline – sections 9(1)(a) of the CIRMP Rules

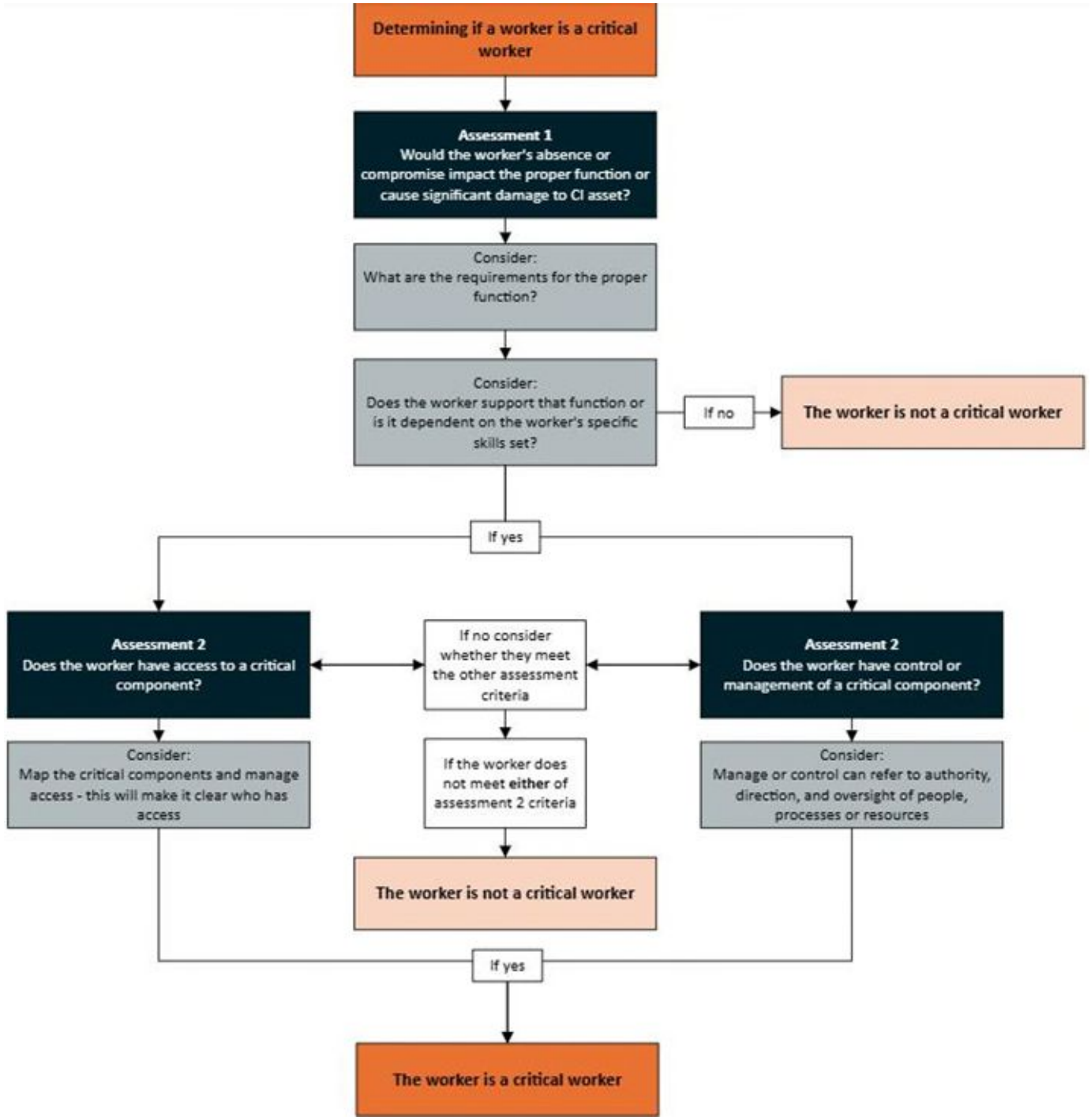
CIRMP enhanced – section 9(1)(a) of the CIRMP Rules

TSRMP – section 12(1)(a) of the TSRMP Rules

Responsible entities with CI assets subject to the baseline or enhanced CIRMP or the TSRMP are required to identify the entity's critical workers.

Critical worker is defined in the **glossary**.

The responsible entity is best placed to assess who constitutes a critical worker for their CI asset. The guidance below can provide responsible entities with a starting point to make that assessment. All parts of the definition of a critical worker must be considered when making this assessment.



Step 1. Determine what is required for the proper function of the asset

Paragraph (b) of the definition of 'critical worker' in section 5 of the SOCI Act outlines that a critical worker is an individual who is an employee, intern, contractor or subcontractor of the responsible entity for a CI asset that is subject to Part 2A of the SOCI Act (referred to in this Chapter as a 'worker') whose absence or compromise would prevent the **proper function** of the asset or could cause significant damage to the asset, as assessed by the responsible entity.

Proper function is described in the **glossary**.

To determine which workers' absence or compromise would prevent the proper function of the asset, the responsible entity will need to assess what the requirements are for that proper function. This will allow the responsible entity to assess which worker capabilities are required to support that function and determine any single points of failure where the function depends on a specific worker(s), skill set, or access.

Once the responsible entity has determined the requirements for the proper function, consider whether this creates a reliance on a:

- specific individual
- unique skill set
- credential holder
- specific decision maker.

Responsible entities may find, in circumstances where knowledge is undocumented or experience-based, that the proper functioning of the asset will require specific workers to be available. In these circumstances, the responsible entity may assess that the absence or compromise of those workers would prevent the proper functioning of the asset.

If the responsible entity has determined that the worker meets the above criteria, then the responsible entity should consider whether the worker also meets the of criteria of paragraph (c) of the definition of 'critical worker' in section 5 of the SOCI Act, which is discussed below.

Step 2. Understand who has access to, or who manages and controls critical components

Paragraph (c) of the definition of 'critical worker' in section 5 of the SOCI Act outlines that the critical worker is a worker that has access to, or control and management of a critical component of the CI asset. The worker must also meet section (b) of the definition of critical worker in section 5, as discussed above, but need not have *both* access to *and* management and control of the critical component.

Step 2.1 Identify critical components

To determine who has access to, or management and control of, the critical components of a CI asset, the responsible entity should identify the critical components of their CI asset. Responsible entities are required to identify physical critical components to comply with their physical security hazard obligations (see **8.2.1** of Chapter 8 – **Physical security and natural hazards**). Responsible entities subject to the enhanced CIRMP are also required to identify and maintain and inventory of their critical systems (see **5.2.1** of Chapter 5 – **Lateral movement hazards**). A CI asset may have other critical components that are not required to be identified as part of complying with these obligations. Effective identification and mapping of all critical components will assist responsible entities in determining who has access to, or management of and control of, critical components.

Step 2.2 Does the worker have access to critical components?

Once the responsible entity has determined what the critical components of the asset are and where they are located, they can build an understanding of who in their workforce has access to those components. Responsible entities should control access to the areas that critical components are located in. in. If access to critical components is not controlled it will be difficult to determine who has access to the critical components, and thus who is a critical worker.

Responsible entities subject to the baseline CIRMP are required to control access to physical critical components (see **8.2.4** of Chapter 8 – **Physical security and natural hazards**) and responsible entities subject to the enhanced CIRMP are required to control access to critical components (see **6.3.2**).

Controlling access may include controlling physical access through swipe cards or controlling remote access through login credentials and multi-factor authentication. Each worker should be issued individual swipe or key cards and login credentials, as shared logins, key cards, and swipe passes make it difficult to understand who has access to critical components and reduces the ability for the responsible entity to determine who is a critical worker.

Step 2.3 Does the worker manage and control the critical components?

Manage and control can refer to exercising authority, direction, or oversight over people, process, or resources. The worker does not need to have access to or physically interact with the critical component to meet this criterion.

A worker may be considered to have authority where they can make decisions that affect how a critical component will function. For example, if they can approve service restoration, system shutdowns, or access controls for other critical workers.

A worker may be considered to have direction if they instruct, guide, or prioritise activities that affect the operation, security, or continuity of a critical component. This could include assigning tasks or setting priorities for critical workers who interact with the critical component. It could also include a worker who determines activities such as the scheduling, incident response, or planned outages of the critical component.

If a worker tells others what must be done, when is should be done, or how it should be done, in relation to the critical component, then that worker likely manages and controls the critical component.

A worker may be considered to have oversight if they have access to strategic or operational information that informs decision-making regarding the critical component. This may be a worker who monitors system performance, security, or reviews reports, alerts or dashboards relating to the critical components. If a worker would be expected to know if something has gone wrong with the critical component, and expected to act on it, they may be considered to manage the critical component.

Having management and control over a critical component can be explicitly stated in a job role or can arise through informal expertise or escalation pathways.

6.2.2 Restrict access to critical workers assessed to be suitable

CIRMP baseline – sections 9(1)(b) of the CIRMP Rules

CIRMP enhanced – section 9(1)(b) of the CIRMP Rules

TSRMP – section 12(1)(b) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP are required to establish and maintain a process or system in the entity's CIRMP to permit access to critical components of the CI asset only where the critical worker has been assessed to be suitable to have such access.

This obligation requires a 4-step process:

Step 1 – The responsible entity should understand the critical components of the asset. The definition of critical components can be found in the **glossary**.

Step 2 – The responsible entity should also understand who the critical workers of the asset are. For information on this see **6.2.1** above.

Step 3 – The responsible entity must then undertake a suitability assessment of each critical worker, which will be detailed below.

Step 4 – Responsible entities subject to the enhanced CIRMP must additionally control access to physical critical components (see **8.2.4** of Chapter 8 – **Physical security and natural hazards**) and multi-factor authentication (see Chapter 4 – **Credential compromise hazards**). All other responsible entities should also consider these access controls as a matter of best practice.

It is likely that the responsible entity will have individuals that have access to critical components that are **not** critical workers. These individuals may not be considered critical workers because their absence or compromise would not prevent the proper function of the asset or cause significant damage to the asset. These individuals are not subject to suitability assessments, however, it is recommended that responsible entities consider the risk these individuals present to the CI asset.

Suitability assessments for responsible entities subject to the enhanced CIRMP vary to the requirements for responsible entities subject to the baseline CIRMP. See **6.2.5** for more information.

6.2.2.1 Identifying if a critical worker is suitable

Responsible entities subject to the baseline CIRMP must establish and maintain a process or system in the entity's CIRMP to permit a critical worker access to critical components of the CI asset *only* where the critical worker has been assessed to be suitable to access the critical component.

Responsible entities may use a background check conducted under the AusCheck scheme to assess whether the critical worker is suitable. A responsible entity may also consider using a commercially available background checking system.

In making a suitability assessment (whether or not that assessment uses a background check conducted under the AusCheck scheme), responsible entities must consider:

a) Any advice obtained through an **AusCheck background check;**
b) Whether permitting a critical worker to have access to the critical components of the CI asset would be **prejudicial to security;** and
c) Any **other information** that may affect the person's suitability to have access to the critical component of the CI asset.

a) Advice obtained through an AusCheck background check

If a responsible entity's CIRMP permits an Auscheck background check, the check must include an assessment of the individual's criminal history and matters relevant to a security assessment of the individual, as well as information including the individual's citizenship, entitlement to work and identity (s 9(3) CIRMP Rules).

When an AusCheck background check of an individual is conducted as permitted by a CIRMP, the Secretary of the Department of Home Affairs must inform the responsible entity of the following matters:

- Whether or not the individual has an unfavourable criminal history.
- Whether or not the individual has an adverse security assessment or qualified security assessment.
- If the Secretary advised the responsible entity of an unfavourable criminal history in relation to a previous background check of the individual – whether there has been a material change to the individual's criminal history.
- Whether the individual has been convicted of a CIRMP-security-relevant offence and, if the individual provides express consent, the details of the offence and any sentence imposed. The definition of a CIRMP-security-relevant offence can be found at regulation 4 of the *AusCheck Regulations 2017*.

The responsible entity must consider whether any of the above circumstances would prevent the critical worker from conducting their role without creating a material risk to the CI asset. An adverse outcome from an AusCheck background check may indicate that the critical worker is not suitable.

An AusCheck background check consists of a:

- Identity verification.
- Nationally coordinated criminal history check.
- Australian Security Intelligence Organisation (ASIO) national security assessment.
- Visa Entitlement Verification Online working rights check (for non-citizens only).

What is an adverse security assessment or a qualified security assessment?

An adverse security assessment is a security assessment in respect of a person that contains:

(a) any opinion or advice, or any qualification of any opinion or advice, or any information, that is or could be prejudicial to the interests of the person, and

(b) a recommendation that prescribed administrative action be taken or not be taken in respect of the person, being a recommendation the implementation of which would be prejudicial to the interests of the person.

A qualified security assessment means a security assessment in respect of a person that meets the above criteria in (a) but does not contain a recommendation of the kind referred to in (b) of the above criteria.

These security assessments are undertaken by the ASIO. These security assessments should be considered by responsible entities as having significant weight against the person's suitability to have access to critical components.

b) What is prejudicial to security?

As part of the suitability assessment responsible entities must consider whether permitting a critical worker to have access to the critical components of the CI asset would be **prejudicial to security.**

For definitions of **prejudicial** and **security** see the **glossary**.

An adverse outcome from an AusCheck background check, or adverse findings about a person arising from suitability assessment measures undertaken by the responsible entity, other than an AusCheck background check, may indicate that allowing the critical worker to have access to critical components would be prejudicial to security. However, minor offences may not meet this bar. The responsible entity should still consider whether the adverse findings, including the adverse outcome from an AusCheck background check, affects the person's suitability to have access to critical components

A finding that the individual having access to critical components may be prejudicial to security is unlikely to be sufficiently mitigated against through other controls (see **6.3.2** for more information on controls). The responsible entity should treat any findings that the worker may be prejudicial to security with significant weight.

c) What is other information that may affect the person's suitability?

When making a suitability assessment, a responsible entity must also consider 'any other information that may affect the person's suitability to have access to the critical components of the CI asset' (s 9(5)(c) of the CIRMP Rules). To determine whether there is any other information that may affect an individual's suitability, the responsible entity should consider undertaking the following checks of an employee:

- identification verification
- qualification and certification checks
- reference checks
- conflict of interest declarations
- right to work checks (visa status)
- criminal history checks, including requesting criminal history records for countries the individual has resided in for more than 12 months
- employment history verification, specifically looking for dismissals for misconduct, or suspicious employment records (for example, frequent changing of roles for no justifiable reason)
- financial probity checks.

When undertaking identification verification responsible entities may consider the **National Identity Proofing Guidelines**[10].

If these checks return an adverse finding, see **6.3.2.1** for more information on controls.

6.2.3 Minimise or eliminate specified material risks

CIRMP baseline – sections 9(1)(c) of the CIRMP Rules

CIRMP enhanced – section 9(1)(c) of the CIRMP Rules

TSRMP – section 12(1)(c) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline and enhanced CIRMP or the TSRMP are required to establish and maintain a process or system in the entity's CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate the material risks outlined below.

6.2.3.1 Risk arising from malicious or negligent employees or contractors

Responsible entities must establish and maintain a process or system in the entity's CIRMP – as far as it is reasonably practicable to do so – to minimise or eliminate the material risks arising from malicious or negligent employees or contractors (section 9(1)(c)(i) of the CIRMP Rules).

Malicious or negligent employees or contractors often have legitimate access to systems and facilities and this makes mitigating or eliminating the risks more difficult. Malicious insiders may deliberately damage operational or information technology systems, leak sensitive information, or disrupt operations. Negligent insiders, while not acting with intent, can create vulnerabilities by mishandling credentials, ignoring security procedures, or failing to report suspicious activities.

[10] https://www.ag.gov.au/national-security/publications/national-identity-proofing-guidelines

Some of the key motivators for malicious insider activity include:

- financial gain
- ideology
- desire for recognition
- foreign allegiance or other divided loyalties
- revenge
- adventure/thill
- ego/self-image
- vulnerability to blackmail
- compulsive or destructive behaviour
- family problems
- negligence
- disgruntlement

See **6.3.2** for best practice mitigations.

6.2.3.2 Risk arising from off-boarding process for outgoing employees and contractors

Responsible entities must establish and maintain a process or system in the entity's CIRMP – as far as it is reasonably practicable to do so – to minimise or eliminate the material risks arising from the off-boarding process for outgoing employees and contractors (section 9(1)(c)(ii) of the CIRMP Rules).

Off-boarding ordinarily refers to the process of disengaging an employee or contractor from an organisation.

Failure to implement effective off-boarding processes can expose CI assets to significant risks, such as:

- **Unauthorised access to systems post-departure** – failure to appropriately revoke system and physical access can lead to sabotage, theft, or general disruption to the operation of a CI asset.
- **Loss of knowledge that is critical to operational continuity** – inadequate information or credential handovers may result in gaps in critical knowledge that could impact the proper function of the CI asset.

This list is not exhaustive. As a matter of best-practice, it is recommended that responsible entities consider whether additional material risks could arise from ineffective off-boarding processes and incorporate these into their CIRMP.

See **6.3.2** for best practice mitigations, and specifically **6.3.2.5** for information on off-boarding processes.

6.2.4 Minimise or eliminate the material risks (enhanced)

Best practice for all responsible entities to consider

CIRMP enhanced – section 9A(2) of the CIRMP Rules

Responsible entities for CI assets subject to the enhanced CIRMP are required to establish and maintain a process or system in the entity's CIRMP to minimise or eliminate material risk. Responsible entities subject to the enhanced CIRMP must minimise or eliminate the material risks outlined below. It is best practice for all responsible entities to consider these risks.

6.2.4.1 Risk associated with unauthorised or unsupervised access to critical components

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain a process or system in the entity's CIRMP to minimise or eliminate the material risk associated with unauthorised or unsupervised access to the critical components (section 9A(2)(a) of the CIRMP Rules).

A failure to implement adequate controls, policies or practices can expose CI assets to risks such as:

- **Sabotage, manipulation, or damage to systems** – unauthorised individuals may intentionally or accidentally alter configurations, disable safety mechanisms, or disrupt operations, leading to outages, equipment failure, or threats to life and safety.
- **Cybersecurity compromise** – unauthorised access to critical systems or components, such as OT, may allow malicious installation of malware, creation of backdoors, the extraction of sensitive data, or actions that facilitate further attacks.
- **Operational disruption** – unauthorised personnel may unintentionally misconfigure critical components, interrupt essential processes, or trigger alarms or shutdowns that impact the continuity of services.
- **Exposure of sensitive or classified information** – unauthorised access can lead to the disclosure of network diagrams, security controls, system credentials, or operational details that could subsequently be exploited by malicious actors.

See **6.3.2** for best practice mitigations. Responsible entities should also consider access controls detailed in **5.2.5.2** of Chapter 5 - **Lateral movement hazards** and physical access controls detailed in **8.3.2.3** of Chapter 8 – **Physical security and natural hazards**.

6.2.4.2 Risk associated with compromise or misuse of credentials and privileged access used by individuals to access the CI asset

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain a process or system in the entity's CIRMP to minimise or eliminate the material risk associated with compromise and misuse of credentials and privileged access used by individuals to access the CI asset (section 9A(2)(b) of the CIRMP Rules).

Privileged accounts may have the ability to view and modify sensitive systems, components, data and information that is critical to the continued reliability of an asset. Credentials form part of a key security boundary to protect a CI asset and should be handled with strong governance throughout their lifecycle.

If these credentials are compromised, misused, or inadequately protected, a CI asset may be exposed to a range of risks, including:

- **Compromise of critical** systems – stolen, guessed, or intercepted credentials can allow adversaries to enter systems under the guise of legitimate users, potentially accessing or altering sensitive operational components.
- **Escalation and exploitation of privileged access** – when elevated accounts are misconfigured, excessive, or insufficiently monitored, individuals may unintentionally or deliberately carry out actions that affect system stability, safety, or availability.
- **Undetected malicious activity** – attackers who rely on valid credentials can blend into normal system traffic, making it difficult to identify harmful behaviour or distinguish legitimate activity from compromise.
- **Integrity and confidentiality breaches** – misuse of privileged accounts may result in unauthorised changes to system settings, security controls, or operational data, reducing trust in the accuracy or reliability of critical processes.
- **Operational disruption or shutdown** – interference with privileged functions can interrupt essential services, diminish situational awareness, or hinder the ability to recover systems during an incident.

See **6.3.2** for best practice mitigations. Responsible entities should also consider mitigations listed in **3.3.2** of Chapter 3 – **Cyber and information security hazards**.

6.2.4.3 Risk associated with access to the CI asset by persons other than critical workers for the CI asset

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain a process or system in the entity's CIRMP to minimise or eliminate the material risk associated with access to the CI asset by persons other than critical workers for the CI asset (section 9A(2)(c) of the CIRMP Rules).

The responsible entity should ensure that risks associated with access to the CI asset by individuals who are not designated as critical workers are appropriately identified, controlled, and monitored. This includes any person who does not require routine access to critical systems, facilities, or operational environments as part of their core duties.

Where non critical workers gain physical or digital access, a CI asset can be exposed to risks such as:

- **Exposure of sensitive operational areas or information** – visitors, vendors, or ancillary staff may unintentionally observe, overhear, or interact with systems or data that could compromise the asset's security if disclosed or misinterpreted.
- **Unintended interference with critical operations** – individuals unfamiliar with procedures or hazards may inadvertently disrupt processes, damage equipment, or trigger safety mechanisms, affecting operational continuity.
- **Introduction of security vulnerabilities** – unsupervised third parties may bring prohibited items, insecure devices, or unverified tools into controlled environments, increasing the potential for malware introduction, system tampering, or contamination of OT.
- **Facilitation of malicious activity** – poorly managed access can create opportunities for social engineering attacks, unauthorised photography, reconnaissance, or deliberate sabotage by individuals with malicious intent.
- **Compromise of safety obligations** – persons lacking relevant training may breach safety protocols, creating conditions that place staff, the public, or the broader environment at risk.

See 6.3.2 for best practice mitigations. Responsible entities should also consider mitigations provided in **3.3.2** of Chapter 3 – **Cyber and information security hazards** and **8.3.2** of Chapter 8 – **Physical security and natural hazards**.

6.2.4.4 Risk arising from incoming or outgoing critical workers

The responsible entity for CI assets subject to the enhanced CIRMP must establish and maintain a process or system in the entity's CIRMP to minimise, mitigate or eliminate the risks associated with incoming or outgoing critical workers (section 9A(2)(d) of the CIRMP Rules).

Incoming workers can present risks due to insufficient vetting, inadequate security training, or poor understanding of site-specific procedures. Workers moving between internal roles or sites may accumulate excessive access privileges over time, leading to privilege creep and breaching the principle of least privilege.

If proper procedures and mitigations are not in place, **outgoing workers** may introduce risk through continued access to facilities and components. Outgoing workers may retain passes, keys or credentials, which increases the risk of unauthorised access. Outgoing workers may intentionally or unintentionally remove sensitive operational, technical, or security information and transfer this to hostile actors. Reliance on highly specialised personnel also creates continuity risk if such workers depart unexpectedly.

Additional risk is introduced by contractors and temporary personnel who have a temporary requirement to access critical components. These workers may be subject to less rigorous or inconsistent vetting and may have lower familiarity with site security requirements, increasing the likelihood of procedural non-compliance or exploitation.

See **6.3.2** for best practice mitigations. Responsible entities should also consider mitigations provided in **3.3.2** of Chapter 3 – **Cyber and information security hazards** and **8.3.2** of Chapter 8 – **Physical security and natural hazards**.

6.2.5 Suitability assessment of critical workers that have access to critical components

Best practice for all responsible entities to consider

CIRMP enhanced – section 9A(3)(a) of the CIRMP Rules

Responsible entities with CI assets subject to the enhanced CIRMP must establish and maintain a process or system in the entity's CIRMP to permit a critical worker access to critical components only where the critical worker has been assessed to be suitable or – if the critical worker is unable to meet the requirements of the suitability assessment – where the responsible entity has outlined in their CIRMP the risk associated with the employment of the critical worker and actions taken, or actions that will be taken as soon as reasonably practicable to do so, to minimise or eliminate the risk to the asset (section 9A(3)(a) of the CIRMP Rules). The assessment as to suitability must be in accordance with section 9A(4) of the CIRMP Rules.

To ensure access to critical components is restricted, considered the physical access controls detailed in **8.3.2.3** of Chapter 8 – **Physical security and natural hazards**, and multi-factor authentication, which can be found in **4.2.3** of Chapter 4 – **Credential compromise hazards**.

A critical worker may be assessed as suitable if:

- An AusCheck background check has been conducted and, following the background check, they have been assessed by the responsible entity as suitable; or
- The critical worker holds a relevant security clearance at the time they were identified to be a critical worker.

If the critical worker is unable to meet the above requirements, then the responsible entity must only permit them access to critical components where the responsible entity has outlined in their CIRMP the risk associated with the employment of the critical worker **and** any actions taken, or that will be taken as soon as reasonably practicable to do so, to minimise or eliminate the material risk to the asset.

To review information on assessing if a critical worker is suitable using an AusCheck background check, see **6.2.2.1**. The responsible entity is required to conduct the AusCheck background check at a minimum every 5 years, if the person requires ongoing access to the critical component (section 9A(5)(c) of the CIRMP Rules).

6.2.5.1 Relevant security clearance

A relevant security clearance is defined in section 3 of the CIRMP Rules as an active security clearance that is:

- Issued by an Australian Government entity that is authorised to undertake security and grant security clearances; and
- At a Negative Vetting 1 level or higher

Where a responsible entity subject to the enhanced CIRMP has a CIRMP that permits a critical worker access to critical components where they have been assessed as being suitable by holding a relevant security clearance, the responsible entity must establish and maintain a process or system in their CIRMP to ensure that, before that clearance lapses or expires, the person:

- Revalidates their relevant security clearance; or
- Obtains an AusCheck background check and is assessed as suitable by the responsible entity.

Critical workers who have a relevant security clearance should declare any changes in circumstances to the issuing body. If the issuing body was AGSVA, changes can be reported via **Reporting changes | Australian Government Security Vetting Agency[11].**

Where a critical worker has applied for, but not yet received, a relevant security clearance they must have an AusCheck background check and be assessed as suitable by the responsible entity, if they are to be permitted access to critical components.

6.2.5.2 Risk assessment of critical worker unable to meet requirements

The CIRMP Rules allow that if a critical worker is unable to meet the suitability requirements – assessed by the responsible entity as suitable, following an AusCheck background check, or hold a relevant security clearance – then a responsible entity must not permit them access to critical components unless their CIRMP outlines the risk associated with the employment of the critical worker and any actions taken, or that will be taken as soon as reasonably practicable to do so, to minimise or eliminate the material risk to the asset.

A critical worker may not be able to meet the requirements due to an adverse finding or a delay in obtaining a clearance or AusCheck background check.

Critical workers have access to critical components and can influence the delivery of the function of the CI asset. There are many risks that may be associated with employing a critical worker without undertaking, or where the critical worker has not cleared, appropriate suitability assessments. Some of these risks include:

- The individual may misrepresent their identity, qualifications, or job history. False identities may mask malicious actors, and unqualified personnel may introduce operational risks.
- The individual may have a conflict of interest which will interfere with their ability to complete the role, or could result in data breaches, biased decision making, or supply chain manipulation.
- The individual may have a prior history of fraud, sabotage, cybercrime, or misconduct. As a result they may be more likely to intentionally compromise systems or networks.
- The individual may be under significant financial strain or experiencing bankruptcy, which may increase their vulnerability to offers from threat groups.

[11] https://www.agsva.gov.au/clearance-holders/reporting-changes

Responsible entities subject to the enhanced CIRMP, who are conducting a risk assessment, must consider all possible risks associated with employing a critical worker who has not been assessed to be suitable following an AusCheck background check or through holding a relevant security clearance. All responsible entities should do this as a matter of best practice. Responsible entities should also consider, as a matter of best practice, risks associated with employing a critical worker, who has returned an adverse finding.

When undertaking this risk assessment, responsible entities should consider undertaking the checks provided at **6.2.2** of this guidance. Undertaking the checks mentioned in **6.2.2** will allow the responsible entity to build an understanding of the types of actions that are required to mitigate the risk of the critical worker having access to critical components.

If the checks return an adverse finding, the responsible entity should consider whether the worker can continue in a role that requires them to be a critical worker, or whether there are mitigations that can lower the risk of the worker to a tolerable level. For information on managing adverse findings see **6.3.2.1**.

6.2.6 Monitor suitability of critical workers

Best practice for all responsible entities to consider

CIRMP enhanced – section 9A(3)(b) of the CIRMP Rules

Responsible entities with CI assets subject to the enhanced CIRMP are required to establish and maintain a process or system in the entity's CIRMP to proactively monitor, identify, and take action in relation to any developments or changes that may affect the suitability of a critical worker.

Responsible entities should consider having regular security reviews for critical workers, as well as trigger based security reviews. The sensitivity of the role will determine how frequent these reviews should be. For example, a critical worker who has a significant level of access to the critical components and is often left alone to work independently should likely have their suitability reviewed more frequently than a worker that has infrequent access and is monitored at all times.

The process for trigger based security reviews should be clearly outlined in a policy or procedure. Potential triggers may include:

- overseas travel
- a security incident
- criminal charges, convictions or court orders
- loss, suspension or restriction of a licence or clearance
- a conflict of interest
- indication that the individual is under financial distress
- association with persons or groups that pose security concern
- significant changes in personal circumstances
- change in geopolitical circumstances.

To assist in monitoring suitability, responsible entities may consider requiring workers to self-disclose information that may impact their suitability.

When an AusCheck background check has been conducted to determine the suitability of a critical worker of a responsible entity subject to the enhanced CIRMP to have access to critical components, and the worker has ongoing access to critical components, then the AusCheck background check must be conducted (at a minimum) every 5 years (section 9A(7)(c) of the CIRMP Rules), unless the worker has obtained a relevant security clearance or higher.

If a change in suitability of a critical worker is detected, the responsible entity should reassess whether the critical worker is still suitable for the role or requires additional mitigations to manage any potential issues.

See **6.3.2.1** for information on best practice approaches to managing adverse findings.

6.3 Best practice for identifying and mitigating risks

This section provides guidance on best practice mitigations for risks associated with personnel hazards. Responsible entities should consider whether these mitigations will assist them in meeting their obligation to– as far as it is reasonably practicable to do so – minimise or eliminate material risks for all hazards and mitigate against the relevant impacts of each hazard on the CI asset (section 7(1)(c) of the CIRMP Rules). The guidance does not comprehensively cover all possible mitigations or risks. The responsible entity must consider additional mitigations as required to address all potential material risks to the CI asset.

6.3.1 Material risks for consideration

Responsible entities must mitigate against the specified material risks in the CIRMP Rules, however they should also consider other possible material risks.

Below are some suggested material risks for consideration. There may be other material risks that are not included in this guidance. It is the responsibility of the responsible entity to identify, eliminate, and minimise these material risks.

Risk Category	Description
Issue motivated groups	Issue-motivated groups (IMGs) are organised collectives that pursue social, political, environmental, or ideological causes. The cause is most often a political reaction to a government or official body, an industrial venture, or a private enterprise. IMGs may consist of environmental activists, 'hacktivists', or union representatives - groups which, while inherently political, aren't officially connected to or represented by a political party. IMGs are not inherently violent; many operate within lawful boundaries. However, a subset may engage in direct action, civil disobedience, or disruptive activities that create risks to personnel and critical infrastructure. Issue motivated groups can include: • Environmental and Climate Activist groups ▪ Animal Rights/Agricultural Activist groups ▪ Anti-government/Anti-authority groups ▪ Digital activism/Hacktivism groups See 6.3.2 for best practice mitigations, and 8.3.2 of Chapter 8 – Physical security and natural hazards.
Overseas travel	Personnel who have access to CI assets are a valuable target for adversaries and foreign intelligence services. Travel exposes staff and their devices to environments where Australian security standards, legal protections, and oversight mechanisms may not apply or be as effective. Personnel may be targeted through surveillance, social engineering, or cyber compromise aimed at gaining unauthorised access to systems or sensitive data. Devices can be tampered with, networks intercepted, or credentials harvested, often without the traveller's awareness. These risks reach beyond the individual traveller. A compromised device or account can provide a pathway into critical infrastructure systems and disrupt operations. See **6.3.2** for best practice mitigations, and **3.3.2** of Chapter 3 – **Cyber and information security hazards**

6.3.2 Treating risk – mitigations and controls

When developing this guidance, the *Australian Government Protective Security Policy Framework* (PSPF) was considered, and some relevant components have been incorporated as best practice. The PSPF prescribes what Australian Government entities must do to protect their people, information and resources, both domestically and internationally.

While the PSPF applies to Australian Government departments and agencies, responsible entities may consider whether its principles and guidance can be adapted to support their own personnel security arrangements. Some mitigations described in the PSPF are specific to government settings and may not be practical or proportionate for industry in all circumstances.

Responsible entities may also consider applying relevant industry standards to support their personnel security practices. Where industry standards are used, entities should be mindful that supplementary controls may still be required to address gaps and ensure their approach is appropriate for their risk environment. Examples include:

- Workforce Screening AS 4811:2022.
- **Australian Government Personnel Security Adjudicative Standard**.

Responsible entities may consider signing up for the **ASIO Outreach Portal**. The portal is available to approved subscribers only and it contains national security reporting and protective security advice on domestic and international issues, including espionage, foreign interference, and politically motivated violence, including terrorism.

6.3.2.1 Managing adverse critical worker suitability findings

When undertaking a suitability assessment as required under the baseline or enhanced CIRMP, the responsible entities may find that an individual has an adverse finding that may impact their ability to be found suitable to have access to critical components. If this occurs, the responsible entity should consider both the significance of the adverse finding and potential mitigations that may allow the individual to continue having access to critical components.

Significance of adverse findings

Adverse findings can vary in significance. An adverse finding that relates to a minor criminal offence that took place many years prior will not have as much weight as an adverse finding that relates to a national security offence. Responsible entities should consider the context of the finding in their assessment. the finding relates.

Some relevant considerations include:

- The length of time since the event took place.
- The relevance of the finding to the individual's work duties and access (for example, a cyber crime would be more relevant to a critical worker who has access to OT).
- Whether there were extenuating circumstances in relation to the event or finding that may reduce the relevance to the CI asset (for example, they declared bankruptcy 5 years ago but have since recovered financially).

Responsible entities should consider all factors relating to the adverse finding and consider the weight they may have in determining whether the individual should have access to a critical component.

Some examples are:

- A worker has several driving offences that took place 5 years ago. These offences are unlikely to have significant weight in the assessment of the worker's suitability. If the worker's job relates to driving, then this offence would have more significant weight.
- A worker has a series of minor burglary offences that took place one year ago. These offences may have some weight in the assessment of the worker's suitability, as it indicates a disregard for law. This would be of significant weight if the worker had access to critical components that have value, such as copper.
- A worker has a cyber crime offence. This may have significant weight, even if the last offence occurred many years prior.
- A worker has inconsistencies in their identity that they cannot explain or reconcile (for example, possibly fraudulent identity documents). This may have significant weight as without a confirmed identity there is no way to know whether they have been convicted of significant offences.

Responsible entities should record these assessments in their CIRMP and update their considerations if circumstances change.

Potential mitigations

If the responsible entity detects an adverse finding during the suitability assessment and they consider the finding not significant enough to find the employee unsuitable, they should consider mitigations to reduce the risk the worker may present.

The nature of the adverse finding will impact the types of mitigations that are required to reduce the risk associated with the critical worker having access to critical components. For example, if the worker has declared bankruptcy or has significant financial debt, the responsible entity should consider restricting access to sensitive financial systems, increase monitoring on the critical worker, and provide financial counselling support.

Generally, the responsible entity should consider the below mitigations:

- Implement dual authorisation controls.
- Increase logging and real time alerts on the individual's system access.
- Ensure least-privilege access with frequent reviews.
- Increase audit frequency on the individual's activities.

This is not an exhaustive list, and the responsible entity should consider the specific risk presented by the critical worker and mitigations tailored to that risk. The additional best practice mitigations listed below and in the other chapters of this guidance will also assist in reducing the potential risk posed by a critical worker with an adverse finding.

If the risk presented by the worker is not able to be appropriately mitigated, then the responsible entity should consider that they are not suitable to hold a position that requires them to be a critical worker.

6.3.2.2 Establishing a positive security culture

Building a positive security culture means creating an environment where people naturally think and act securely, not because they're forced to, but because they understand the value and feel responsible for it. Improving the security culture of an organisation can help staff be more security conscious and vigilant in their day-to-day business.

A positive culture transforms employees from potential risks into active participants in security. When staff internalise security as part of "how we work here", this works towards reducing reliance on oversight.

When employees trust the organisation and feel safe to speak up

- They may report suspicious behaviour, policy breaches, or mistakes early.
- Issues such as insider threats, coercion attempts, or accidental data exposure may be caught before they escalate.

A positive security culture is characterised by

- Leadership modelling secure behaviours.
- Workers who feel responsible for protecting information and systems.
- High levels of reporting (mistakes, suspicious behaviour, near misses).
- Low tolerance for risky shortcuts.
- Clear, simple security processes embedded in everyday work.
- A positive security culture can improve security outcomes across all hazards. By making it clear what the expectations are, and building an environment where workers are comfortable calling out inappropriate behaviour, staff become another layer of defence against risk. A positive security culture may improve:
- Cyber security outcomes as workers may report unusual emails or interactions online.
- Physical security as workers may call out unusual or unexpected persons on the property or in secure areas.
- Personnel security as it may provide a level of oversight on personnel behaviour that would otherwise be unachievable.

6.3.2.3 Security awareness training

Workers are an important layer of protection for CI assets. When workers are engaged and security conscious they can provide surveillance, reporting, and early detection of threats. Security awareness training can help staff to recognise and respond to behaviours, activities and indicators that there is threat or potential impact to the CI asset.

Security awareness training should apply to all employees, contractors, and third parties with access to the CI asset, systems, or sensitive information. Training should also be risk and role appropriate. A worker who has more privilege, control, or unsupervised access should receive additional training. Consider whether specific roles present different risks that require specific training. For example, someone working in ICT may require more in-depth cyber security training.

Workers that are subject to a suitability assessment should receive training on maintaining these checks and declarable circumstances to allow for monitoring of the validity of their suitability.

Below are some examples of what training should cover. The list is not exhaustive, and responsible entities should undertake a detailed assessment of what other topics staff may require training on. At a minimum, training should cover:

- Password hygiene and credential protection.
- Physical access controls and procedures (such as swipe pass use, tailgating, etc.).
- Social engineering techniques.
- Cyber security awareness.
- Identification of suspicious behaviour and trusted insider threat indicators.
- Natural hazard awareness and response.
- Procedures for responding to and reporting incidents.
- Security risks associated with remote or hybrid work.

Training should adopt an all hazards approach and reinforce behaviours that support security across multiple threat vectors.

Security awareness training should be embedded into worker inductions and regularly reinforced through refresher sessions. When a procedure is changed, workers should be appropriately informed and trained to ensure continued compliance.

Consider running drills and practice exercises to test the effectiveness of security awareness training programs.

It is critical that workers are supported to report concerns without fear of reprisal. Reporting pathways should be clearly defined, confidential where appropriate, and well understood.

Robust security awareness training underpins the effectiveness of security policies and procedures. Without a clear understanding of expectations and warning signs, workers cannot be relied upon to consistently apply the controls in place.

6.3.2.4 Knowledge transfer and record keeping procedures

Knowledge transfer and record keeping procedures are important for maintaining continuity and resilience when workers leave an organisation or transition between roles. Without structured handover arrangements, organisations risk the loss of critical knowledge or documentation.

Clear and well-defined knowledge transfer expectations can help to ensure that operational knowledge and decision-making information are not retained by a sole individual. This is particularly important for roles that require specialist expertise or privileged systems access.

Record keeping procedures should be embedded in workforce management processes and additional steps should be taken to transfer knowledge to effectively manage resignation, role change, extended leave, or contract termination.

Effective knowledge transfer practices may require departing or transitioning staff to:

- Document key responsibilities, workflows, and dependencies.
- Record critical operational processes and decisions.
- Highlight known risks, issues or unresolved matters.
- Ensure all documentation is current, accurate, and stored in approved organisational systems rather than personal files or informal repositories.
- Participate in structured handover discussions with managers or incoming staff.
- Where possible, avoid dependencies on individual staff members.

Attention should be given to environments where documentation practices are inconsistent or where knowledge is heavily experience based. Capturing this information reduces reliance on informal knowledge networks and supports continuity during both planned and unplanned workforce changes.

Knowledge transfer should be supported by good record keeping practices, including clear ownership of documentation, version control, and defined storage locations. Information relevant to the operation, maintenance, and security of CI assets should be readily accessible to authorised personnel and protected in accordance with security and information management policies.

By formalising knowledge transfer and record keeping processes, organisations strengthen their operational resilience, reduce reliance on individual staff members, and ensure continuity of critical functions during workforce transitions.

6.3.2.5 Off-boarding processes

Off-boarding processes help organisations maintain security and operational continuity when workers depart. Proper off-boarding processes help to ensure that access, assets and information are managed in a controlled and accountable way. Effective off-boarding reduces the risk of unauthorised access, accidental information loss or intentional misuse during or after an employee's departure. These procedures work alongside knowledge transfer procedures and insider threat monitoring to ensure that departures do not introduce vulnerabilities into the organisation.

Effective off-boarding procedures may include:

- The immediate revocation of digital and physical access when a staff member leaves the organisation.
- Expedited removal of access in cases of involuntary termination.
- Return of IT assets, identification passes, and other equipment.
- Verification that all organisational information is appropriately stored
- Verification that any organisational information stored on personal devices or accounts has been destroyed.
- Audit procedures to ensure there are no dormant accounts from previous employees.

Good off-boarding procedures require coordination between different areas within an organisation. There needs to be adequate communication between human resources, line managers, IT departments, security teams, and finance teams. This communication ensures a seamless process. If areas do not appropriately communicate, removal of accesses and asset management may be delayed. This can create a significant risk during a time where employees may be more susceptible to targeting from malicious actors.

6.3.2.6 Insider threat monitoring

Insider threat monitoring helps to detect and respond to behaviours or activities that may indicate a risk from current, incoming or departing personnel. Monitoring should focus on identifying unusual or unauthorised actions, such as unexpected data downloads, attempts to access systems outside normal duties or unexplained changes to system configurations.

Clear access management processes, regular review of user permissions and established reporting pathways help staff and managers respond effectively to concerning behaviour. Implementing technical controls such as activity logging, automated alerts for high risk actions, and routine audits further strengthens the ability to detect potential insider threats early. Together, these measures may assist in timely intervention and reduce the likelihood or impact of an insider driven security incident.

6.3.2.7 Clean desk policies

Clean desk and clear screen practices can help to protect classified information from accidental exposure or unauthorised access. These measures help reduce the likelihood that sensitive material is overlooked, mishandled or observed by individuals without an appropriate clearance or need to know. Maintaining an organised and secure work environment reduces the risk of compromise during routine operations or unexpected events.

Responsible entities should consider ensuring that their staff only keep essential documents on their desks while working and ensure that all information, whether hardcopy, electronic media or portable devices, is stored securely when not in use. It is recommended that informal recording methods, such as sticky notes, not be used for classified information. Whiteboards should be cleared when left unattended and storage containers locked whenever not actively in use. Keys, access tokens and other enabling items should be kept secure, such as in the user's custody or an approved key safe.

It is recommended that classified material not be visible to individuals without the appropriate need to know. Measures such as minimising documents on screens, locking computers when away from the workstation (even briefly) and securing physical copies help mitigate against accidental exposure or unauthorised access. Other portable or attractive items should also be secured to prevent theft, misuse or accidental exposure.

6.3.2.8 Visitor procedures

Visitor procedures help organisations maintain control over who can access their premises and reduce the risk of unauthorised individuals observing, accessing or interfering with sensitive information, assets or operations. Clear processes ensure that workers understand their responsibilities when hosting visitors and that all visits are managed in a consistent and secure manner. These procedures are particularly important in environments where valuable or sensitive information is stored, as even brief unsupervised access may result in accidental exposure or deliberate misuse.

Effective visitor procedures may include requirements for visitors to present current photo identification, have their details recorded in a visitor register and be signed in by an authorised staff member. Visitors should only enter the workplace with approval from the relevant work area and wear a visitor pass while on premises.

To minimise security risks, responsible entities should consider escorting all visitors at all times and providing them with a clear explanation of site security expectations and the consequences of non-compliance. Additionally, it is recommended that visitors not be permitted to connect personal electronic devices to the entity's networks or systems, including for charging, as this may introduce cyber security threats. These measures may help reduce the likelihood of inadvertent exposure, unauthorised access or misuse of resources, and support a controlled and secure operating environment.

Responsible entities should consider potential risks arising from foreign delegates visiting the CI asset.

6.3.2.9 Overseas travel policies

It is recommended that responsible entities consider the risk presented by workers travelling overseas for business and recreational purposes. Responsible entities could assess the potential consequences of a compromise occurring during or after travel and implement layered controls to prevent, detect, and contain incidents. Regular review and testing of these controls ensure they remain effective as the threat environment evolves

When developing a travel policy, consider how the precautions may vary based on the circumstances of the travel. For example:

- Whether the worker is travelling for business or recreation.
- The level of access to systems, networks, or data that the worker has.
- The country that is being visited.

To effectively manage overseas travel risks, responsible entities should establish clear and enforceable controls that apply at each stage of travel. A structured approach covering **before, during**, and **after** travel ensures personnel are prepared, protected and monitored in accordance with the risk management program. Below are potential mitigations for each stage of the journey.

Before travelling

By managing risk before the travel occurs, responsible entities can prevent an incident that may compromise their devices, data, or network. By preparing workers, configuring secure devices, and limited access to sensitive data, entities can significantly reduce the likelihood of compromise once staff are offshore. Potential mitigations include:

- Workers informing their employer that they are travelling overseas, the duration of the trip, and the countries that will be visited.
- Establishing a level of systems access workers can maintain while overseas, which may vary if they are travelling for business or recreational purposes. Systems access should be as limited as possible, while still being able to perform necessary functions.
- Regular training sessions for workers that include best practice strategies and behaviours for staff overseas. Including training on identifying suspicious, ongoing, unusual and persistent behaviour which may indicate they are being targeted for malicious action.
- As needed, requiring workers to attend pre-travel briefings that provide relevant information for the country they will be visiting. If an employee is travelling to a high risk country, it is recommended that a travel briefing is mandatory.
- Consider instructing workers not to take device that have access to any corporate systems or data when travelling to high risk countries.
- Ensure employees' devices have up to date software, operating systems, and applications. This will improve the devices ability to defend against malware.
- Ensure devices have appropriate PIN, biometric locks, and multi-factor authentication on applications.

During travel

This is the highest risk phase of the travel journey. Personnel are operating in potentially hostile cyber environments, where monitoring, interception, or social engineering are more likely. Active vigilance, technical controls, and situational awareness are essential to maintain security.

- Consider requiring employees to use connection controls. This may include the use of virtual private networks, or prohibiting access through public Wi-Fi or unsanctioned SIM cards.
- Monitor access for unusual login activity from overseas. Ensure multi-factor authentication is in use.
- Remind overseas workers that devices and communications may be monitored at all times.
- Ensure workers are diligent in retaining possession of their devices at all times or are storing them securely.
- Require reporting of suspicious, ongoing, unusual or persistent behaviour or contact while overseas.

After travel

Returning devices and data should be treated as potentially compromised. Post travel screening, isolation, and reporting ensure any intrusion attempts are detected early and are not spread into domestic systems. Responsible entities could:

- Require ICT screening before reconnecting devices to corporate systems.
- Mandate that workers declare any suspected compromise, loss, or unusual activity.

Together, these stages form a lifecycle approach to travel security that supports both operational mitigation of risk, and compliance with the SOCI Act's risk management program requirements.

6.4 Worked example – CIRMP entry

Below is an example of a personnel hazard, the assessment a responsible entity may record to determine whether the hazard is a material risk, and the controls in place to manage the risk and the impact of the eventuation of the risk. This example is a suggestion, and there is no requirement for responsible entities to record their assessments in this way.

Field	Example Response
Hazard	Official overseas travel by a critical worker with their work issued devices.
Asset(s) / Site	Network Operations Centre (NOC) – **Site B** (coordinates delivery of the essential services). Includes access to key systems used to monitor and manage the service.
Scenario	A critical worker travels overseas and retains remote access to systems used to monitor and manage the service. The worker is targeted (such as through social engineering or device compromise) and credentials that allow access to systems are compromised.
Why this is material	▪ Compromise of a critical worker (or their device/credentials) can enable malicious activity that appears "legitimate" and is harder to detect. ▪ Malicious actors may use compromised devices or credentials to disrupt the proper function of the CI asset. ▪ Access to the credentials may impact Site B which contains systems/areas where interference can cause extended outages and broader downstream impacts.
Relevant impact mapping	**Availability:** service interruption or slowdown due to unauthorised actions. **Integrity:** unauthorised configuration changes or operational actions taken using compromised credentials or under coercion. **Confidentiality:** unauthorised access to sensitive operational information.
Evidence supporting likelihood	▪ Country information available on Smartraveller.gov.au (Reviewed — Mar 2026) ▪ Prior security review identified inconsistent travel notification and variable controls for overseas access (Reviewed — Jan 2026). ▪ Near miss: unusual overseas login attempt during prior travel period (Reviewed — Nov 2025)
Key dependencies / interdependencies **(Include here the cascading impact that may result from the realisation of the hazards)**	Dependent on availability, integrity, and confidentiality of systems in Site B: ▪ Corporate network. ▪ Surveillance and monitoring of critical components. ▪ Remote access to critical componentry. ▪ As a result of impact, critical systems must operate independently until the responsible team can undertake recovery and restoration of the compromised system.
Controls — Preparedness	▪ Travel policy with clear before / during / after travel requirements for critical workers, including declaration and briefings for higher-risk travel. ▪ Playbook for suspected travel-related compromise that includes containment steps, credential resets, device screening, and escalation. ▪ Tabletop exercise: "overseas travel + suspected compromise + operational disruption" (Scheduled — Aug 2026).
Controls — Prevent / minimise likelihood	▪ Limit systems access while overseas to the minimum required (risk- and role-based) and apply stronger sign-in controls for remote/privileged access. ▪ Pre-travel briefings for higher-risk travel. ▪ Avoid taking devices that provide direct access to sensitive systems for higher-risk destinations.

Controls — Impact mitigation	▪ Rapid containment: disable accounts/badges immediately when suspicious activity is detected. ▪ Post-travel controls: ICT screening before reconnecting devices to corporate systems where required by policy.
Owners / status / timeframes	▪ Travel declaration + briefing process — Security Lead — Implemented; refresh annually. ▪ Monitoring/log review — Security Operations Lead — In progress; Sep 2026. ▪ Post-travel screening workflow — ICT Operations Lead — Planned; Oct 2026.
Residual risk and acceptance	▪ Residual risk assessed as medium due to reliance unavoidable travel requirements for specialist roles. ▪ Risk acceptance approved by the Risk Committee (Jun 2026).
Review cadence / triggers	Formal review annually as part of CIRMP review. Trigger review after: ▪ Any suspected compromise, coercion attempt, or travel-related security incident or near miss. ▪ Significant change to remote access arrangements or overseas travel profile. ▪ Audit findings indicating gaps in travel declaration, briefing, monitoring or post-travel controls.
Supporting material	▪ Travel policy and evidence of completion (briefings, declarations). ▪ List of critical workers with travel notification records.

Table of contents: Chapter 7

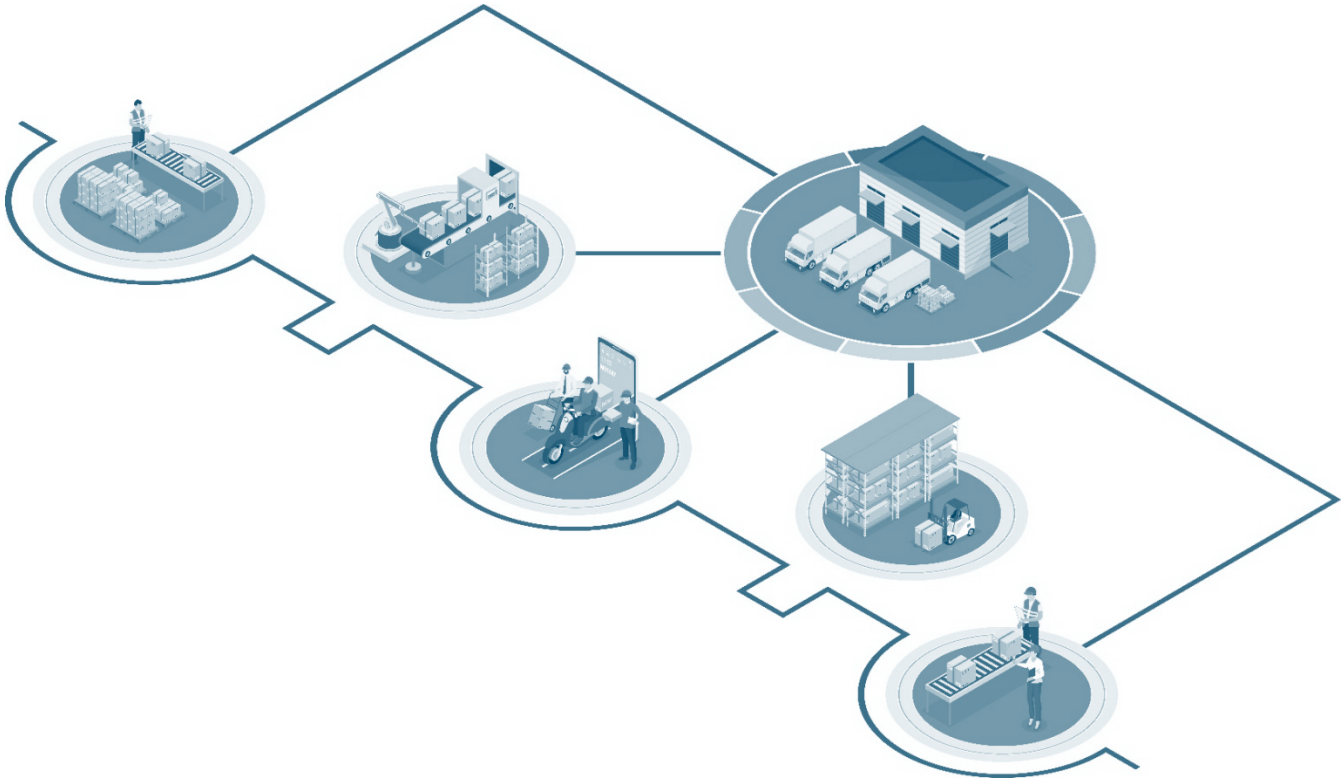
7.1 Obligations for managing supply chain hazards 92
7.2 Meeting the obligations in practice 93
7.2.1 Minimise or eliminate a material risk, and mitigate the relevant impact 93
7.2.1.1 Risk arising from unauthorised access, interference, or exploitation of a CI asset's supply chain 95
7.2.1.2 Misuse of privileged access to CI assets by any provider in the supply chain 95
7.2.1.3 Disruption of the asset due to an issue in the supply chain 96
7.2.1.4 Threats to people, assets, equipment, products, services, and intellectual property within supply chains 97
7.2.1.5 Risks arising from major suppliers 97
7.2.1.6 Failure or lowered capacity of other assets and entities in the supply chain 98
7.2.2 Supply chain mapping for major suppliers and critical components 99
7.2.3 Vendor assessment for proposed or existing major suppliers 101
7.3 Best practice for identifying and mitigating risks 102
7.3.1 Material risks for consideration 103
7.3.2 Treating risk – mitigations and controls 103
7.3.2.1 Recording provenance of critical components 103
7.3.2.2 Supplier diversification 103
7.3.2.3 Supplier arrangements and contract design 104
7.3.2.4 Strategic stockholding (buffer stock) 104
7.3.2.5 Supply chain risk planning 105
7.3.2.6 Substitution 105
7.3.2.7 Industry engagement during disruption 105
7.3.2.8 Scenario exercises and stress testing 106
7.3.2.9 Identifying onshore supplier options 106
7.4 How to map supply chains 106
7.4.1 Define scope and approach 107
7.4.2 Conduct mapping 107
7.4.2.1 Identify and document key parties 107
7.4.2.2 Identify gaps 109
7.4.2.3 Illustrate the supply chain 109
7.4.3 Relying on third-party contractors to map your supply chain 111
7.4.3.1 Internal buy in and support 111
7.4.3.2 Establishing clear expectations 111
7.4.3.3 Software 111
7.4.4 Identify supply chain vulnerabilities 111
7.4.4.1 Assess exposure and vulnerabilities 111
7.4.4.2 Assess criticality 114
7.4.5 Residual risk 118
7.5 Illustrative case studies 120
7.6 Worked Example – CIRMP Entry 121

7. Supply chain hazards

Critical infrastructure operators rely on suppliers to provide equipment, software, specialised skills, services and surge capacity needed to support the safe and effective operation of their assets.

For many organisations, these dependencies are an unavoidable part of doing business. However, weaknesses or security deficiencies in suppliers - whether in their products, practices, or contractual and operational arrangements - can undermine the security and integrity of critical infrastructure, particularly if they remain undetected for extended periods.

These risks are amplified by the complex network of interdependencies between critical assets across sectors. A disruption or compromise in the supply chain of one asset can have cascading impacts across multiple sectors, including where suppliers themselves depend on upstream providers. Concentration of key suppliers - where a small number of providers directly or indirectly support multiple critical assets - can mean a single supplier incident may disrupt multiple critical services across the economy and pose significant risks to Australia's national security.



7.1 Obligations for managing supply chain hazards

The table below outlines the obligations in the CIRMP Rules in relation to supply chain hazards. It outlines whether the obligations apply to responsible entities subject to the baseline and/or enhanced CIRMP requirements and/or TSRMP requirements.

The obligations are expanded on later in this chapter.

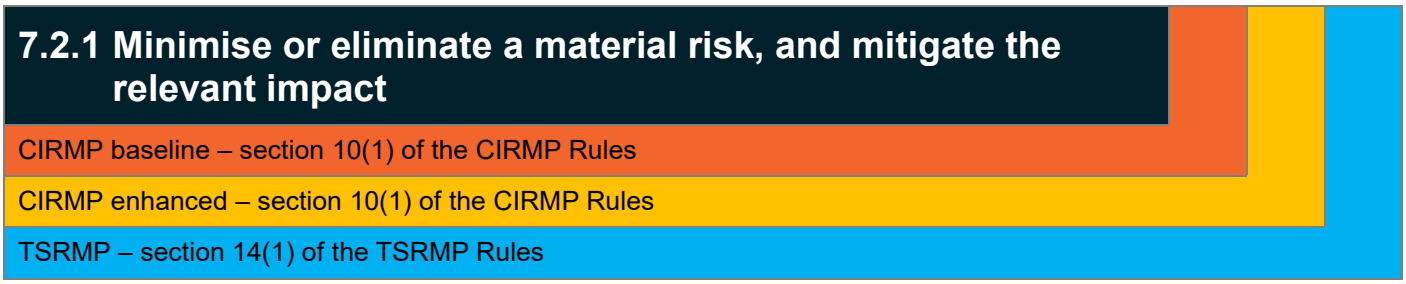
Supply chain hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Responsible entities must establish and maintain a process or system in the entity's CIRMP to - as far as it reasonably practicable to do so - minimise or eliminate the following material risks: (i) Unauthorised access, interference or exploitation of the asset's supply chain; (ii) Misuse of privileged access to the asset by any provider in the supply chain; (iii) Disruption of the asset due to an issue in the supply chain; (iv) Arising from threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; (v) Arising from major suppliers; and (vi) Any failure of lowered capacity of other assets and entity's supply chain. The responsible entity must also - as far as it reasonably practicable to do so - mitigate the relevant impact of a supply chain hazard on the asset	s 10(1)	s 10(1)	s 14(1)
Responsible entities must establish and maintain a system or process in the entity's CIRMP to map their supply chain for major suppliers and critical systems across their supply chains. The entity's CIRMP must: identify risks in the entity's supply chain that may affect the availability, integrity, reliability or confidentiality of critical components or compromise business critical data; and identify the maximum acceptable outage for the CI asset or any of its critical components arising from the disruption to the entity's supply chain; and as far as is reasonably practicable to do so—include measures to minimise or eliminate those risks, or mitigate the impact of an outage that exceeds the maximum acceptable outage.		s 10A(2) s 10A(3)	
Responsible entities must establish and maintain a system or process in the entity's CIRMP to assess the risks associated with an existing or proposed major supplier for the CI asset. The system or process must identify, for each existing or proposed major supplier: in relation to foreign ownership, control or influence (FOCI) risks—legislative or other legal requirements to which the supplier is subject to; and restrictions, sanctions or other impediments affecting the jurisdiction to which the entity may be subject to; and the access, influence and control the supplier has over the CI asset in connection with the product or service the supplier provides; and the extent to which the matters in paragraphs (a), (b) and (c) together may present a material risk for the CI asset, or could exceed a maximum acceptable outage of the service or product provided by the supplier; and		s 10A(4) s 10A(5)	

Supply chain hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
as far as reasonably practicable to do so— steps to minimise or eliminate material risks and mitigate the relevant impact of the hazard on the CI asset.			

Timeframes for compliance are explained in Chapter 1 – **Introduction to the critical infrastructure risk management program (CIRMP)** at **1.5**

7.2 Meeting the obligations in practice

7.2.1 Minimise or eliminate a material risk, and mitigate the relevant impact



Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP are required to establish and maintain in the entity's CIRMP a process or system to – as far as it is reasonably practicable to do so – minimise or eliminate material risks in relation to supply chain hazards and mitigate a relevant impact of a supply chain hazard on a CI asset.

As identified in subsection 10(1) of the CIRMP Rules, these material risks include:

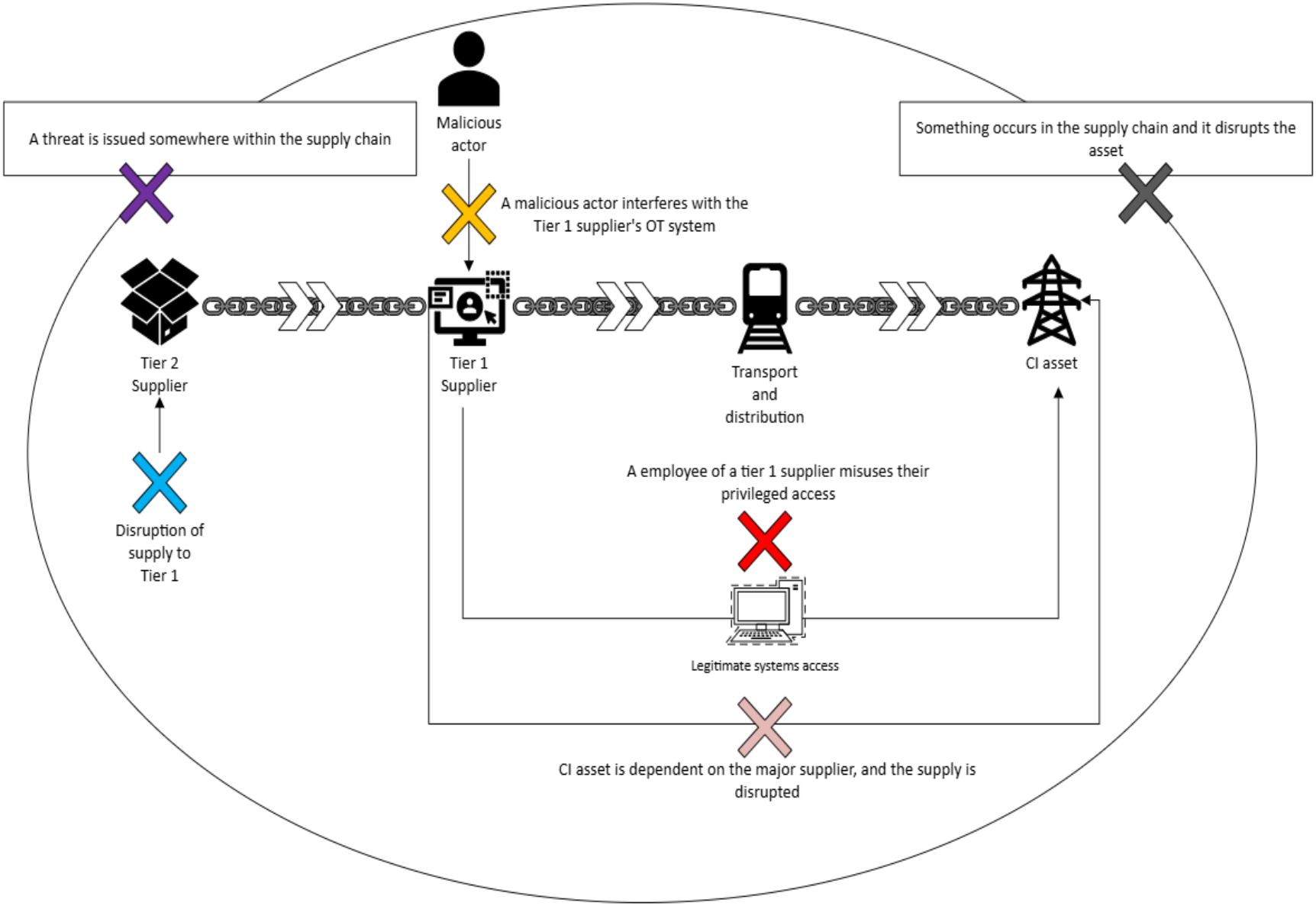
- unauthorised access to, interference with or exploitation of the asset's supply chain
- misuse of privileged access by providers in the supply chain
- disruption of a CI asset due to issues in the supply chain
- material risks arising from threats to people, assets, equipment, products, services, distribution channels and intellectual property within supply chains
- material risks arising from major suppliers
- any failure or reduced capacity of other assets or entities within the responsible entity's supply chain.

Responsible entities subject to only the baseline CIRMP (and not the enhance CIRMP) or the TSRMP are not required to undertake supply chain mapping for major suppliers and critical components (as per section 10A(2) of the CIRMP Rules). However, it is strongly recommended that all responsible entities consider undertaking some level of supply chain mapping. This will allow responsible entities to manage risk associated with their supply chain by developing a thorough understanding of the way risk is introduced in their supply chain. For guidance on how to map a supply chain, see **7.4** of this chapter.

Responsible entities must also – as far as it is reasonably practicable to do so – take steps to mitigate the relevant impact of a supply chain hazard on the asset.

The graphic below depicts a CI asset's supply chain, and the way material risks may interact or occur along the continuum of the supply chain. Supply chain material risks can involve:

- Actions against a supplier in the supply chain.
- Actions from a supplier against the CI asset.
- A general disruption somewhere along the continuum.



7.2.1.1 Unauthorised access, interference, or exploitation of a CI asset's supply chain

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must establish and maintain a process in the entity's CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate the material risk of unauthorised access, interference or exploitation of a CI asset's supply chain (section 10(1)(i) of the CIRMP Rules and section 14(1)(i) of the TSRMP Rules).

The risk of unauthorised access, interference or exploitation of a supply chain may arise from malicious actors, compromised suppliers, foreign interference, or weakness in third-party security practices. A failure to appropriately manage these risks may lead to impacts on the CI asset and have cascading effects on the reliability of the CI asset.

Suppliers often have legitimate access (whether physical or virtual) to a CI asset's critical components, critical systems or business critical data as part of performing services or providing key products. This access may be leveraged by the supplier or malicious actors (either with the complicity of the supplier or covertly) to interfere with the asset in ways that undermine its security or effective operation.

Responsible entities should consider the definitions of unauthorised access, interference, and exploitation provided in the **glossary**.

These events may also trigger a responsible entity's Notification of Cyber Security Incident (NCSI) reporting obligation – see **NCSI Guidance**[12].

For information on mitigations for material risks see **7.3.2** of this chapter.

Some of the mitigations provided in other chapters will help the responsible entity to identify when unauthorised access, interference or exploitation has occurred – see **3.3.2** of Chapter 3 – **Cyber and information security hazards** and **6.3.2** of Chapter 6 – **Personnel Hazards**

7.2.1.2 Misuse of privileged access to CI assets by any provider in the supply chain

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must establish and maintain a process in the entity's CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate the material risk of misuse of privileged access to CI assets by any provider in the supply chain (section 10(1)(ii) of the CIRMP Rules and section 14(1)(ii) of the TSRMP Rules).

Suppliers may require elevated levels of access to systems, data, components or physical facilities that form part of a CI asset. This may include maintenance contractors, managed service providers, or software and hardware vendors providing technical or operational support.

Privileged access presents a risk as it may enable suppliers to bypass or override normal safeguards. Where access is misused - whether intentionally or through a compromise of a supplier by another party - this can cause significant harm to the CI asset.

[12] https://authors.cisc.gov.au/resources-subsite/Documents/ncsi-guidance.pdf

Cyber misuse of privileged access

From a cyber perspective, misuse of privileged access may include:

- Installing malicious code or unauthorised software on systems or devices that are key to critical asset operations.
- Exploiting security vulnerabilities to establish unauthorised or backdoor access into critical systems or networks for the supplier or third parties.
- Disabling critical systems, hardware or software.
- Accessing, exfiltrating, or manipulating sensitive data, including unauthorised use of AI.
- Tampering with logs or monitoring systems to conceal activity or falsify information.

Responsible entities should consider whether their suppliers have a cyber security framework that protects their ability to deliver their product or services. Responsible entities should consider implementing a contractual obligation for suppliers to ensure they have and maintain a cyber security framework that achieves an appropriate level of security. Responsible entities may consider including the ability to audit or review this framework where required.

Physical misuse of privileged access

From a physical perspective, misuse of privileged access may include:

- Acts of sabotage, theft, or deliberate damage to key equipment or components.
- On-site tampering that creates safety, reliability, or operational risks.
- Conducting illicit on-site surveillance to gather sensitive operational information. This information may then be shared with other parties, used to cause competitive harms or pre-position for future attacks against the asset

For information on mitigations for material risks see **7.3.2** of this chapter.

7.2.1.3 Disruption of the asset due to an issue in the supply chain

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must establish and maintain a process in the entity's CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate the material risk of disruption of the asset due to an issue in the supply chain (section 10(1)(iii) of the CIRMP Rules and section 14(1)(iii) of the TSRMP Rules).

This material risk may refer to any interruption, degradation, or loss of the CI asset's ability to maintain its proper function as a direct or indirect result of a supply chain issue. Disruptions may:

- Affect critical components or supporting systems.
- Reduce the asset's ability to deliver essential services safely and reliably.
- Be short term or prolonged.
- Cause cascading impacts to interconnected systems, sectors, or services.

Examples of disruptions may include:

- Outages or degraded performance of critical systems due to vulnerabilities or failures in cloud services, hardware or software used upstream in an asset's supply chain.
- Reduced or complete loss of availability of vital inputs for operations including spare parts from manufacturers, fuel, chemicals, or other key consumables.
- Loss of access to key staff such as contractors, vendors, support or maintenance personnel, limiting an asset's ability to continue to sustain operations at full capacity.
- Delays or blockages in key transport and logistics pathways (such as geopolitical events or natural hazards), limiting the delivery of vital materials or components to the asset.

Disruption of the asset can arise from many different issues in the supply chain. A thorough understanding of the suppliers in the supply chain provides the responsible entity with the ability to anticipate potential issues. Responsible entities subject to the enhanced CIRMP are obligated to undertake vendor risk assessments (as outlined in section 10A(4) of the CIRMP Rules) and map their supply chains (as outlined in section 10A(3) of the CIRMP Rules). Adherence to these obligations will assist entities in addressing this material risk. It is best practice for all responsible entities to consider these obligations. Read about them at **7.2.3** and **7.4** of this chapter.

For information on mitigations for material risks see **7.3.2** of this chapter.

7.2.1.4 Threats to people, assets, equipment, products, services, and intellectual property within supply chains

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must establish and maintain a process in the entity's CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate the material risk of threats to people, assets, equipment, products, services, and intellectual property within supply chains (section 10(1)(iv) of the CIRMP Rules and section 14(1)(iv) of the TSRMP Rules).

Threats to any element of a CI asset's supply chain can lead to material risks that can potentially impair the CI asset itself.



The below are some possible ways to think about the threats to people, assets and equipment, products and services, and intellectual property:

- **People** – insider threats (for example key contractors or suppliers are bribed, influenced, or otherwise have their integrity compromised), loss of key individuals in the supply chain (for example, absence of technical support contractors due to illness, natural hazard or geopolitical hazard) or targeted attacks against key individuals (for example kidnapping, physical harm, coercion or harassment of contractors or suppliers).
- **Assets and equipment** – theft, sabotage or damage (whether deliberate or through natural causes) to key components or supplies held by or supplied by vendors that are needed to operate the asset.
- **Products and services** – degradation in the quality of vital materials needed by the asset (for example counterfeit components or contaminated fuel), or compromises to key software and hardware (for example, software or hardware used by a CI asset is compromised with malicious code).
- **Intellectual property (IP)** – theft or misuse of sensitive IP that suppliers have access to as part of the services or products they provide to an asset (for example, research, designs or proprietary technology pertaining to the asset). IP can also be obtained by malicious actors under the guise of what appears to be normal business engagements, such as fact-finding during acquisitions and mergers.

For information on mitigations for material risks see **7.3.2** of this chapter.

7.2.1.5 Risks arising from major suppliers

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must establish and maintain a process in the entity's CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate the material risk arising from major suppliers (section 10(1)(v) of the CIRMP Rules and section 14(1)(v) of the TSRMP Rules).

Identifying major suppliers

Major suppliers are those that, by virtue of the nature of the product or service they offer, have a significant influence over the security of a CI asset.

Responsible entities should consider the definitions provided in the **glossary** for major supplier, security, vendor, and significant influence.

Whether an entity is a major supplier depends on the product or service the vendor offers. Assessing a vendor only by their size or value of the vendor will not determine whether they are a major supplier.

A major supplier is one who, by the nature of the good(s) or service(s) they offer, can significantly influence whether the asset is protected from security threats

The vendor does not need to be able to control the CI asset to be a major supplier. Rather, it needs to be able to significantly influence the CI asset's ability to respond to and recover from security threats. A supplier may have significant influence over the security of the CI asset where it can:

- enable or prevent detection of threats
- introduce vulnerabilities
- control critical functions or systems
- access business critical data.

When determining whether a vendor meets the threshold of a major supplier, some possible considerations are provided below:

- Does the vendor supply an essential good or service that supports core operations?
- Is there anyone who has potential adverse influence and control over a vendor?
- Would the absence of the good or service supplied by the vendor significantly impede the ability of the CI asset to continue functioning or supplying critical services?
- What level of exposure does the vendor have to the CI asset? For example, do they have privileged access to key systems, data or physical facilities?
- If the vendor were to fail or cease operations, how easily could they be replaced?
- How long would it take to transition to another vendor or adjust operating models, and could this occur without a disruption to operations or significant financial or logistical impacts?
- Would a compromise of the vendor create a significant operational or security risk for the CI asset?
- If the supplier were compromised, coerced, or failed to deliver, would it increase the risk of espionage, sabotage, or other national security threats to the CI asset?

Consideration of the above factors may help responsible entities determine whether a vendor could have a significant influence over the security of a CI asset. If so, then they should be treated as a major supplier.

Consider the risks major suppliers present

Major suppliers can represent a disproportionate source of risk to critical infrastructure. Some examples of scenarios where a major supplier risk may exist include:

- **Suppliers who are fundamental to key operational processes** – they may provide operational technology, hardware, software or services which an asset cannot function without (such as specialist maintenance firms, fuel or chemical suppliers, cloud monitoring services or communication links that support telemetry functions)
- **Suppliers with a significant influence on security** – they may have privileged remote or on-site access to key systems, data or facilities, or have the ability to control or change key operational processes.
- **Suppliers who create a systemic dependency** – this could include suppliers who form part of an ecosystem that is inherently fragile or single-source (for example, they may provide components from a single country or region which many organisations rely on). Geopolitical issues (such as wars, export bans or natural disasters) affecting the supplier may cripple the operation of multiple CI assets.
- **Suppliers with access to sensitive data or information flows** – they may store, process or transmit operational, security or customer data, creating a risk of unauthorised access, data exfiltration or misuse that could undermine system integrity.
- **Suppliers subject to extra-territorial judicial obligations** – they may be required under the laws of foreign countries to provide access to data, systems, services or information to foreign governments. This may result in unauthorised disclosure of sensitive information, disruption to operations, or influence over critical functions.

For information on mitigations for material risks see **7.3.2** of this chapter.

7.2.1.6 Failure or lowered capacity of other assets and entities in the supply chain

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must establish and maintain a process in the entity's CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate any failure or lowered capacity of other assets and entities in the supply chain (section 10(1)(vi) of the CIRMP Rules and section 14(1)(vi) of the TSRMP Rules).

Risks to the functioning of a CI asset can arise where upstream or downstream parties in the supply chain experience a failure or lowered capacity, even where there is no direct compromise to the asset itself. These risks could include degraded operations, temporary shutdowns, or increased safety risks for staff or the community at large. Examples include:

- **Major IT outages** – such as to cloud or hosting services that provide key functionality such as system monitoring, backups or support for control systems.
- **Utilities failures** – this could include water, electricity or telecommunications outages that affect the ability of a CI asset to function.
- **Transport and logistics failures** – this could lead to delays in the provision of critical resources such as spare parts, fuel or chemicals needed for operations. It could also lead to delays in the supply of a key product produced by the asset to the broader community.
- **Worker shortages** – this could include temporary or ongoing staffing issues (such as unexpected resignations or industrial strikes) in supply chain partners that provide technical support or other key services.
- **Downstream bottlenecks** – this could include waste processing facilities for water treatment or distribution network service providers in electricity markets. A failure of these downstream parties can mean that a CI asset must either reduce output or shut down entirely.

For information on mitigations for material risks see **7.3.2** of this chapter.

7.2.2 Supply chain mapping for major suppliers and critical components

Best practice for all responsible entities to consider

CIRMP enhanced – section 10A(2) and 10A(3) of the CIRMP Rules

Responsible entities subject to the enhanced CIRMP must establish and maintain a process or system within their CIRMP to map their supply chain for major suppliers and critical components across their supply chains. This extends across both physical and cyber supply chains.

The mapping process in the responsible entity's CIRMP must:

- Identify vulnerabilities and risks within the supply chain that could affect the CI asset.
- Identify the maximum acceptable outage for the CI asset, and for any critical systems, components, major suppliers or providers that support the asset.
- Include within their CIRMP - so far as it is reasonably practicable - measures to mitigate identified vulnerabilities and risks, or to mitigate the impacts of an outage exceeding a maximum acceptable outage.

Detailed guidance on supply chain hazard mitigations (**7.3.2**), supply chain mapping (**7.4**), and identifying vulnerabilities and risk in supply chain (**7.4.4**) are provided in this guidance. These listed sections are best practice guidance

Responsible entities should also ensure they consider their cyber supply chain when undertaking this obligation. Responsible entities should consider accessing the Australian Signals Directorate's Australian Cyber Security Centre's **Managing cyber supply chains | Cyber.gov.au guidance**[13].

Maximum acceptable outage is defined in the **glossary**. A thorough understanding of the maximum acceptable outage will allow for the appropriate implementation of this obligation.

Governance and accountability

Responsible entities should assign clear ownership for the maintenance of their supply chain mapping. The accountable role should be responsible for ensuring mapping is updated in accordance with agreed schedules or event-based triggers, and for escalating material changes or risks through appropriate governance channels.

To what extent should the supply chain be mapped?

This obligation requires responsible entities to map the supply chain for their major suppliers and critical systems. For guidance on how to map your Tier 1, 2, and N suppliers, see **7.4.2**.

For information on identifying major suppliers see **7.2.1.5** of this chapter.

For information on identifying critical systems see **5.2.1** of Chapter 5 - **Lateral movement hazards**.

Responsible entities are only expected to map the supply chains associated with major suppliers and critical systems. It is best practice for responsible entities to map these supply chains to their Tier N suppliers were possible.

[13] https://www.cyber.gov.au/business-government/supplier-cyber-risk-management/managing-cyber-supply-chains

When undertaking the initial supply chain mapping process, it is recommended that responsible entities undertake a prioritisation model informed by risk. Responsible entities should start by mapping all Tier 1 suppliers to their major suppliers and critical systems. Once this has been done, they should consider the risks that may be present for these suppliers and prioritise accordingly. Some risks that may be considered as higher priority may include:

- A single point of failure has been identified.
- A geographic concentration of suppliers, particularly in a region subject to extrajudicial direction.
- A known low level of cyber security maturity.
- A fragmented or poorly understood supply chain.
- A heavy reliance on the supplier.

Once responsible entities have determined the level of risk, it is recommended that they seek to prioritise mapping Tier 2 and N suppliers for the higher risk vendors first. Once this is complete, the responsible entity can then move to mapping lower risk vendors to Tier 2 and N levels.

Reviewing and updating the supply chain map

Responsible entities should consider establishing governance arrangements with their key suppliers to support timely and proactive updates to supply chain information.

Responsible entities should consider establishing an internal cadence for updating their supply chain map that aligns with the agreed supplier update cycle. They should also consider implementing trigger based updating.

Scheduled updates

Responsible entities should consider:

- Updating their supply chain map on a regular schedule that corresponds with key supplier information reviews.
- Validating and incorporating supplier-provided updates during each review cycle.

To maintain accuracy over time, responsible entities should consider integrating supply chain mapping updates into existing business processes, such as:

- supplier onboarding and sourcing decisions
- contract management and renewals
- risk and incident management processes
- change management for operational or strategic initiatives.

This integration helps ensure supply chain mapping remains a living process rather than a one-off exercise.

Trigger based updates

In addition to scheduled updates, responsible entities should consider requiring ad hoc updates to their supply chain map when triggered by events, including but not limited to:

- Changes to suppliers (onboarding, offboarding, or substitution).
- Contract renewals or material contract amendments.
- Supplier incidents (such as operational disruptions, financial distress, cyber or safety incidents).
- Major internal operational changes, such as new products, services, markets, or significant changes in volume or sourcing strategy.

Responsible entities should also consider:

- Arranging information-sharing expectations with key suppliers, including the requirement to maintain visibility over upstream supply chain dependencies.
- Requiring suppliers to proactively notify the responsible entity of material changes to their supply chains, such as changes in subcontractors, production or service locations, logistics arrangements, ownership, or any issues that may affect continuity of supply.
- Clearly define what constitutes a “material change” to ensure consistent reporting.
- Establish a defined cadence (for example, quarterly or bi-annual) for suppliers to review, confirm, and update their supply chain information.

Where appropriate, these expectations should be documented in contractual arrangements or supplier codes of conduct.

7.2.3 Vendor assessment for proposed or existing major suppliers

Best practice for all responsible entities to consider

CIRMP enhanced – section 10A(4) and 10A(5) of the CIRMP Rules

Responsible entities for CI assets subject to the enhanced CIRMP must establish and maintain a process in the entity's CIRMP to assess risks associated with an existing or proposed major supplier for their CI asset.

Major suppliers, particularly those with significant access, integration or ability to control or influence assets can introduce risks that may affect the reliability of a CI asset. These risks may arise from the major supplier's ownership structure, operating environment, or the nature of the services they provide.

This assessment must consider, and the responsible entity's CIRMP must identify, a range of supplier-related risk factors, including:

- FOCI risks, including legislative or other legal requirements the supplier is subject to.
- Restrictions, sanctions or other impediments affecting the jurisdiction and which the entity may be subject to.
- The access, influence and control the supplier has over the CI asset in connection with the products or services provided by the supplier.
- Whether these factors collectively give rise to material risks to the CI asset or could exceed the maximum acceptable outage of the supplier's service or product.

This obligation does not require a responsible entity to cease using a vendor because they present a risk. It requires responsible entities to consider the risk and apply mitigations. The responsible entity may determine that the most practical mitigation is to cease use; this is entirely at the discretion of the responsible entity.

New Suppliers

When onboarding a new supplier, the responsible entity should first consider whether this new supplier will be considered a major supplier, see **7.2.1.5** for an explanation of that term. This determination will inform the level of assessment and ongoing oversight required.

The onboarding phase provides an opportunity for responsible entities to embed controls at the beginning of the supplier relationship. Responsible entities should consider incorporating contractual provisions that support their obligations under the SOCI Act. This may include requiring the supplier to:

- Notify the responsible entity of any change in circumstance that may affect their suitability as a major supplier, such as:
    - A change in ownership structure.
    - A change in legal or regulatory frameworks within the supplier's jurisdiction.
    - Geopolitical developments that may affect the supplier's operation, reliability or alignment with Australian interests.
    - Significant operational, financial, or reputational issues affecting the supplier.
    - Changes to the scope of services or level of access provided to the supplier.
- Comply with specified security, resilience and assurance requirements.
- Participate in audits, risk assessments, or information sharing arrangements.

Embedding these clauses early supports a proactive approach to risk management and reduces the reliance on mitigating controls later in the supplier relationship.

Existing suppliers

Responsible entities should take a risk-based approach to the implementation of this obligation. Where a responsible entity has a large number of major suppliers, it may not be practicable to assess all suppliers simultaneously. In these circumstances, responsible entities may prioritise based on:

- Criticality of the supplier to the proper function of the CI asset.
- The level of access, influence, or control the supplier has.
- The likelihood that the supplier may present a heightened risk based on known factors (such as geographic location, conflicts of interest, geopolitical environment).
- Whether the supplier could have a relevant impact on the CI asset.

By undertaking this prioritisation process the responsible entity can focus efforts on suppliers that pose the greatest potential risk to the asset first. Responsible entities are required to assess **all** major suppliers within the relevant

timeframes, see **1.5** on Chapter 1 - **Introduction to the critical infrastructure risk management program (CIRMP)** for timeframes.

FOCI model contract clauses

The Department of Home Affairs' FOCI model contract clauses are available to help responsible entities manage and mitigate FOCI risks in procurement. They are designed to support a range of procurement activities, including tendering, contracting and contract management.

The model clauses are optional. Responsible entities should select and apply the clauses that are appropriate to the level of FOCI risk identified with a particular procurement activity. Responsible entities may use the clauses to embed practical safeguards into procurement arrangements, and to respond to changes in the supply chain over the life of a contract.

Further information is available at - **Foreign Ownership, Control or Influence (FOCI) Risk Assessment Guidance[14].**

Download - **FOCI model clauses for industry[15].**

Ongoing assessment and review

Responsible entities are encouraged to assess suppliers on a regular and ongoing basis, as the supplier's risk profile may change over time. A supplier that is assessed as being low risk may later have a change of circumstances that could increase their potential risk. Regular reassessment helps ensure that changes in circumstances that result in risk are identified and managed in a timely manner.

Responsible entities are encouraged to have regular, scheduled reviews and trigger based reviews of their suppliers. Contracts may restrict the responsible entity from terminating or altering the relationship with the vendor, regardless of findings from the review. In these cases, responsible entities should consider whether alternative mitigations can be applied to reduce the likelihood or impact of supply chain disruption.

Responsible entities should consider embedding contract clauses that require suppliers to update them on information that may trigger a review. Some potential triggers for undertaking a trigger based risk assessment may include:

- A change in ownership structure.
- A change in legal or regulatory frameworks within the supplier's jurisdiction.
- Geopolitical developments that may affect the supplier's operation, reliability or alignment with Australian interests.
- Significant operational, financial, or reputational issues affecting the supplier.
- Changes to the scope of services or level of access provided to the supplier.

This allows responsible entities to maintain an understanding of the supplier risks and ensure their approach remains effective over time.

We encourage responsible entities to consider using the Foreign Ownership, Control or Influence (FOCI) Risk Assessment Guidance when considering their vendor assessment obligation.

This guidance is considered best practice for all responsible entities.

[14] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/foreign-ownership-control-or-influence-risk-assessment-guidance

[15] https://www.homeaffairs.gov.au/nat-security/files/foci-model-clauses-industry.pdf

7.3 Best practice for identifying and mitigating risks

This section provides guidance on best practice mitigations for risks associated with supply chain hazards. Responsible entities should consider whether these mitigations will assist them in meeting their obligation to minimise or eliminate material risks relating to supply chain hazards and/or mitigate against relevant impacts of those hazards (as required by section 10(1) of the CIRMP Rules). The guidance does not comprehensively cover all possible mitigations or risks. The responsible entity must consider additional mitigations as required to address all potential material risks to the CI asset.

7.3.1 Material risks for consideration

Responsible entities must mitigate against the specified material risks in the CIRMP Rules, however they should also consider other possible material risks.

Below are some suggested material risks for consideration. There may be other material risks that are not included in this guidance. It is the responsibility of the responsible entity to identify, eliminate, and minimise these material risks.

Risk Category	Description
Tier 2 and Tier N supplier concentration	Limited visibility of lower tier suppliers can mask critical dependencies on single source providers or geographically concentrated production. Disruption to raw material can propagate upstream and disrupt supply continuity, which ultimately impacts Tier 1 suppliers and the responsible entity. Supply chain mapping, as detailed at **7.4** can assist in identifying this risk and is mandatory for responsible entities subject to the enhanced CIRMP.
Specialised workforce and skills shortages	A dependence on a highly specialised or certified personnel for manufacturing, maintenance, or logistics operations can create a workforce disruption either directly in the CI asset, or in suppliers. A labour shortage can impact the productivity of suppliers and disrupt the function of the CI asset, or a lack of skilled workers can make it difficult to deliver the proper function of the CI asset.

7.3.2 Treating risk – mitigations and controls

7.3.2.1 Recording provenance of critical components

Responsible entities should consider incorporating a process or system to record the movements of critical components in and out of their control. This includes maintaining visibility of a component's ownership, location, and usage throughout its lifecycle.

The movement of components between environments of differing trust levels can undermine established security controls (such as movement of devices from IT to OT environments). Responsible entities should consider implementing appropriate controls to manage provenance and ensure that components are not introduced into trusted environments without adequate assurance.

Any instance of components leaving a responsible entity's control (such as maintenance, repair, or disposal) introduces additional supply chain risk. Responsible entities should consider applying compensating controls in such scenarios, particularly where components are transferred outside of Australia, to maintain assurance over the security and integrity of the CI asset. This can include maintaining a list of movements, checking components prior to reintegrating them into the CI asset environment, and ensuring vendors who have contact with the componentry have been appropriately considered for the risk they may present.

7.3.2.2 Supplier diversification

Avoiding excessive reliance on a single supplier, market or region can help reduce exposure to supply chain disruptions, particularly for inputs that are critical to ongoing operations. Concentration risks can build gradually over time as sourcing decisions are optimised for cost, scale or efficiency, and may not be immediately visible without periodic review.

In practice, supplier diversification does not require duplicating supply for all inputs. Many responsible entities focus on identifying where reliance on a single supplier, geography or market would result in a material disruption if supply were interrupted, and where viable alternatives could reasonably be developed. This may include considering how quickly alternative suppliers could be activated, and whether switching would be feasible in terms of cost, quality or lead times.

Supplier diversification strategies should be proportionate to the level of risk and reviewed as business operations evolve. In some cases, maintaining relationships with potential alternative suppliers, even where they are not used under normal conditions, can improve preparedness and reduce response times during disruption.

In considering supplier diversification, responsible entities may reflect on:

- whether critical inputs rely on a single supplier, country or region
- how quickly alternative suppliers could be accessed if needed
- whether cost-driven sourcing decisions are increasing concentration risk
- whether supplier concentration has changed as the business has grown or diversified.

7.3.2.3 Supplier arrangements and contract design

Supplier arrangements and contracts can play an important role in managing supply chain risks, particularly where responsible entities rely on major suppliers or inputs that are critical to the operation of the asset. Contractual and governance arrangements can help clarify expectations, improve information flows, and strengthen preparedness for disruption.

In practice, responsible entities may use supplier arrangements to support resilience by addressing issues such as surge capacity, access to alternative supply, and communication during incidents. This can include considering how quickly suppliers can respond to unexpected demand or disruption, whether contingency or reserve capacity is available, and how information about emerging risks or constraints is shared. Clear communication protocols and regular engagement with major suppliers can also help build a shared understanding of vulnerabilities and response options.

Supplier arrangements should be proportionate to the level of risk and the nature of the dependency. Over time, reviewing supplier performance and preparedness can help responsible entities identify where additional safeguards are warranted, or where diversification or alternative arrangements may be more effective in managing risk.

In considering supplier arrangements, responsible entities may reflect on:

- whether key inputs are supported by more than one active supplier
- how supplier contracts or agreements address surge, contingency or reserve capacity
- whether communication protocols are in place for incidents or emerging constraints
- the extent to which supplier arrangements have been tested or reviewed in practice.

7.3.2.4 Strategic stockholding (buffer stock)

In some circumstances, holding inventory can be an effective way to manage supply chain risks, particularly for inputs that are critical to operations and difficult to substitute in the short term. Strategic stockholding can provide a buffer against temporary disruptions, buying time for alternative arrangements or recovery actions to take effect.

The appropriateness of stockholding will vary depending on factors such as lead times, storage requirements, costs, and the likelihood and duration of disruption. For some responsible entities, this may involve prioritising stock for inputs with long lead times or limited substitutability, or establishing minimum and maximum stock levels to balance resilience benefits against cost and obsolescence risks.

Stockholding strategies should be considered alongside other mitigation measures, rather than in isolation. Regular review of inventory levels, usage patterns and supplier conditions can help ensure that stockholding remains aligned with the entity's risk profile and operational needs.

In considering strategic stockholding, responsible entities may reflect on:

- which inputs are most critical to sustaining operations during disruption
- whether those inputs have substitutes or long lead times
- how stock levels are monitored and adjusted over time
- whether changes in supplier behaviour or market conditions affect stockholding needs.

7.3.2.5 Supply chain risk planning

Building flexibility into operations can help businesses recover more quickly when supply disruptions occur. Supply chain risk planning focuses on identifying how operations could adapt under stress, rather than assuming that supply chains will always function as expected.

For many entities, this involves considering in advance how inputs, outputs or operating models could be adjusted if key supplies are disrupted. This may include identifying realistic options to pivot production, temporarily modify services, or adjust demand, and ensuring that these options are reflected in broader business continuity and risk management planning.

Planning for flexibility is most effective when it is grounded in an understanding of actual supply chain vulnerabilities. Integrating supply chain risks into existing planning processes can help ensure that response options are practical, understood by decision-makers, and capable of being activated when needed.

In considering supply chain risk planning, responsible entities may reflect on:

- whether operations can be adjusted if supply is disrupted
- what would be required to pivot production or services
- whether flexibility is built into business continuity planning
- whether assumptions about adaptability have been tested or reviewed.

7.3.2.6 Substitution

Planning for acceptable substitutes can help maintain continuity during periods of supply shortage, particularly where disruptions are expected to be temporary. Substitution may involve using alternative inputs, products or processes that allow operations to continue, even if at reduced efficiency or scope.

Effective substitution planning requires careful consideration of feasibility and impacts. Substitutes may raise issues relating to safety, quality, regulatory approvals, or customer expectations, and may require changes to processes or communications. As a result, substitution is often most effective when treated as a temporary measure rather than a permanent solution.

Identifying and documenting substitution options in advance can help reduce delays and uncertainty during disruption. Periodic review of substitution options can also help ensure they remain viable as products, regulations and market conditions change.

In considering substitution, responsible entities may reflect on:

- whether acceptable substitutes exist for critical inputs
- whether substitutes would meet safety, quality and regulatory requirements
- what operational or approval changes substitution would require
- how substitution would be communicated to customers or partners.

7.3.2.7 Industry engagement during disruption

In some circumstances, engagement with industry peers can help reduce collective supply risks, particularly during widespread or systemic disruptions. Where appropriate and lawful, coordination through industry associations or established forums can support information sharing and more effective management of shortages.

Engagement is most effective when communication pathways are established in advance of disruption. Sharing high-level information about constraints, demand pressures or recovery timelines can help reduce uncertainty and avoid actions that may unintentionally worsen shortages, such as uncoordinated purchasing or hoarding behaviour.

Any coordination between competitors should be undertaken with careful consideration of legal and competition requirements. Where coordination may raise competition law issues, entities may wish to seek early advice and be aware of available mechanisms, such as ACCC authorisation, that can support coordination in the public interest during crises.

In considering industry engagement, responsible entities may reflect on:

- whether uncoordinated actions could exacerbate shortages
- whether industry forums or peak bodies exist for engagement
- whether communication pathways are established in advance
- whether legal and competition considerations are understood.

7.3.2.8 Scenario exercises and stress testing

Scenario exercises can help an entity test how they would respond to plausible supply disruptions and identify gaps in preparedness. These exercises are not intended to predict specific events, but to improve decision-making, clarify roles and refine triggers for mitigation actions.

Many entities focus scenario exercises on a small number of critical inputs or services, testing how existing mitigations, such as alternate suppliers, buffer stock or substitution options, would perform under stress. Exercises can also help clarify who is responsible for key decisions during disruption and when escalation is required.

Lessons learned from scenario exercises can be used to strengthen business continuity planning, supplier arrangements and mitigation strategies over time. Even relatively simple tabletop exercises can provide valuable insights into organisational readiness.

In considering scenario exercises, entities may reflect on:

- whether responses to prolonged disruptions have been tested
- whether decision-making roles and escalation triggers are clear
- whether existing mitigations would be sufficient under stress
- how lessons learned are captured and acted on.

7.3.2.9 Identifying onshore supplier options

Where feasible, domestic supply options may help reduce exposure to disruptions affecting international supply chains. Onshore suppliers can sometimes provide shorter lead times, reduced exposure to border or transport disruptions, or greater visibility during crises.

Considering onshore options does not imply that domestic supply will always be the most efficient or cost-effective choice. In practice, some entities identify domestic suppliers as back-up or supplementary options, even where they are unable to meet full demand under normal conditions. Early engagement, pre-qualification or trial orders can help reduce activation time if onshore supply is needed during disruption.

The relevance of onshore options will vary by sector and input, and should be considered as part of a broader, risk-based approach to supply chain resilience.

In considering onshore supplier options, responsible entities may reflect on:

- whether reliance on overseas supply creates material exposure
- whether domestic suppliers exist for critical inputs or substitutes
- what barriers limit use of onshore supply (such as cost, scale, or specifications)
- whether relationships with potential onshore suppliers are established in advance.

7.4 How to map supply chains

Understanding how a CI asset depends on its supply chain is central to managing supply chain hazards. Supply chains are often complex and interconnected, and disruption at a single point can have cascading impacts on critical systems and operations.

For CIRMP purposes, supply chain mapping is intended to support risk-based decision-making, rather than to document every supplier or transaction in detail. Many responsible entities focus first on developing a clear view of the inputs, suppliers and logistics that are critical to their operations, particularly where there is reliance on major suppliers, limited substitutability, long lead times, or exposure to external hazards such as natural disasters, geopolitical tensions or transport chokepoints.

Improved visibility can help entities identify key dependencies and single points of failure, understand which vulnerabilities would have the most significant operational or commercial impacts if disrupted, and prioritise mitigation actions in a way that balances resilience benefits against cost and feasibility. Supply chain information should be reviewed periodically and kept current to reflect changes in operations, suppliers and the broader risk environment.

In developing supply chain visibility, responsible entities may consider:

- whether they have a clear view of critical inputs, suppliers and logistics supporting operations
- where key dependencies, bottlenecks or concentration risks exist across the supply chain
- which disruptions would have the greatest operational or commercial impact
- how improved visibility can help prioritise mitigation efforts on a cost-benefit basis.

7.4.1 Define scope and approach

The first step in conducting supply chain mapping is to clearly define both the scope and the approach that will be undertaken. It is important to note that this activity is contextual to critical infrastructure and mapping may not need to be all-encompassing. Responsible entities should focus on essential goods and services required to operate their critical asset(s) and deliver their core offerings.

7.4.1.1 Define scope

Before mapping is conducted, two key scope parameters should be decided:

- The products or services to be mapped.
- The depth to which mapping will go (i.e. Tier 1, Tier 2, Tier 3). Tiers reflect the level within the supply chain and describe the directness of the relationship or connection to your business.
    - Tier 1 suppliers provide direct services or goods to your entity.
    - Tier 2 refers to the suppliers to your Tier 1 suppliers.
    - Tier 3 + refers to the suppliers to the Tier 2 suppliers, and so on. This can continue down as many layers as required and can be referred to as n-tier mapping.

To assist in defining the scope of the mapping to be undertaken, consider the following:

- What are the processes necessary to produce and deliver your essential goods and / or services?
- Are there any critical interdependencies between your essential goods and services?
- Who are the vendors that supply the services and products your critical asset relies upon to operate? This may include raw materials, packaging, transportation and management software.
- What essential processes and third parties do your vendors rely upon to provide you with goods and services?

7.4.1.2 Define approach

There is no one set approach for mapping your supply chain. The approach will depend on the industry, complexity of the supply chain(s) to be mapped and the determined scope. Two main guiding approaches can be used.

- **Option 1: by key product or service (*preferred).*** This is the option will be used as the framing of this chapter to explain subsequent steps of the mapping process.
- **Option 2: by major suppliers or contracts.** This option is more suitable if an entire service or product is outsourced, or a major supplier is responsible for a large proportion of different products or services for your entity.

7.4.2 Conduct mapping

Once the approach and scope have been defined, mapping of the supply chain can commence. The below sections outline an example of how to work through mapping using a structured approach. However, it is important to note the mapping process is iterative and does not always follow a clear linear structure.

7.4.2.1 Identify and document key parties

The identification and documentation of suppliers is an iterative process, **and not all required information may be available immediately**. It is important to document the information in a format that easily captures linkages that can be used to create a visualisation later.

Step 1. Identify Tier 1 Suppliers

For products and services selected as part of scope definition, the first step is to identify all direct suppliers (both contracted and non-contracted). When identifying suppliers, it is important to document key information that will be used to determine relationships and vulnerabilities. *Table 1* captures the types of data that could be collected.

Table 1: Supply chain mapping data collection template

Data type	Data required	Purpose
Supplier name	Legal entity name (and trading name, if different)	Unique identification of suppliers and consistent naming across contracts, systems and tiers.
Engagement type	Contracted or non-contracted	Clarifies governance, leverage and available controls (such as contractual obligations, assurance rights).
Contract type	Contract vehicle/type (for example standing offer, pricing-based, scope-based)	Supports assessment of commercial structure, flexibility, and how easily changes can occur.
Contract period	Start date, end date, renewal and extension options (termination notice periods if available)	Enables planning for renewals, continuity risk at contract end, and timing of assurance activities.
Goods or services supplied	Description of goods and services and upstream product/service category	Helps define dependencies and ease of mapping for products/services in scope.
Share of supply	Percentage of volume/spend supplied (and whether sole/primary supplier)	Quantifies concentration and easy identification of single points of failure.
Mode of delivery	How the goods/services are supplied (such as digital, air, rail, road, ship)	Useful for determining how goods and services are received and options to pivot in case of supply disruptions.
Capacity	Normal capacity and maximum capacity, surge/ramp-up time, constraints/inputs needed to increase output	Indicates a possibility to increase supply during disruptions, demand spikes, or when other suppliers fail.
Exclusivity clauses	Any exclusivity or non-compete terms affecting alternative sourcing	Identifies constraints on switching suppliers and potential barriers to resilience mitigations.
Contingency Clauses	Any contingency clauses and criteria for execution (such as force majeure)	Understand continuation of supply in case of disruption.
Operating location(s)	Headquarters locations and operating sites (such as warehouses, manufacturing, data centres)	Supports geographic risk analysis (clustering, hazards, jurisdictional exposure) and visualisation of the network.
Ownership details	Parent entity/ultimate beneficial owner (where available), overseas/state ownership indicators	Informs jurisdictional, governance and sovereignty considerations and geopolitical risks.
Known downstream suppliers	For tier 2+, list downstream suppliers that goods and services are provided to.	Used for mapping connections and relationships
Known upstream suppliers	Where applicable, list upstream suppliers relevant to the goods/services provided	Used for mapping connections and relationships.

Step 2. Identify Tier 2 suppliers

Mapping beyond Tier 1 becomes more challenging. For each of the identified Tier 1 suppliers, there will be a requirement to identify their suppliers relevant to your product or service. This step will not always be straightforward, and suppliers may be hesitant to be fully transparent on their commercial arrangements, subsequently presenting opacity in the upstream supply chain.

To undertake this mapping, you will be required to engage and collaborate with your Tier 1 suppliers to obtain the necessary information. To assist in this process, consider the following when engaging with Tier 1 suppliers:

- Engaging in a preliminary conversation, being transparent in your objectives for wanting to understand their supply chain.
- Providing a template and requesting completion of the necessary information.
- Leveraging any contractual clauses requiring suppliers to disclose any subcontractors or suppliers relevant to the products or services being provided. If this is not a current contractual requirement, consider amending your contract to include it, where appropriate.
- Establishing regular governance forums to ensure ongoing discussions and visibility to any changes to the Tier 2 network.

When information is obtained on downstream suppliers, document the information is the same format as for Tier 1 suppliers (see *Table 1* for reference).

Step 3. N tiers (if possible)

This may require extensive stakeholder engagement and changing governance processes to extract the necessary information. Close engagement with upstream suppliers will be required, and direct engagement with lower tier suppliers may not be possible, unless permission is granted. Where data is available, collect and document it in the same format as other tiers.

7.4.2.2 Identify gaps

Data gaps may consist of incomplete supplier information or unknown suppliers for certain stages of the supply chain. Identifying gaps in supplier information is important to ensure clear action can be taken to amend or mitigate said gaps.

As you are conducting the iterative supply chain mapping process, document gaps in supplier information in a tracker and note what is missing, relevance and the remediation options (such as contract documentation, supplier questionnaire, further engagement). Ensure to implement a review mechanism so gaps are resolved as the map is iterated over time.

If a gap cannot be resolved, flag it as a risk against the most relevant upstream supplier(s). For example, if Tier 3 details cannot be obtained, record the gap against the associated Tier 2 supplier and, where appropriate, the Tier 1 supplier. This ensures that future reviews of the supplier data and network diagram clearly show where dependencies exist, but information is incomplete.

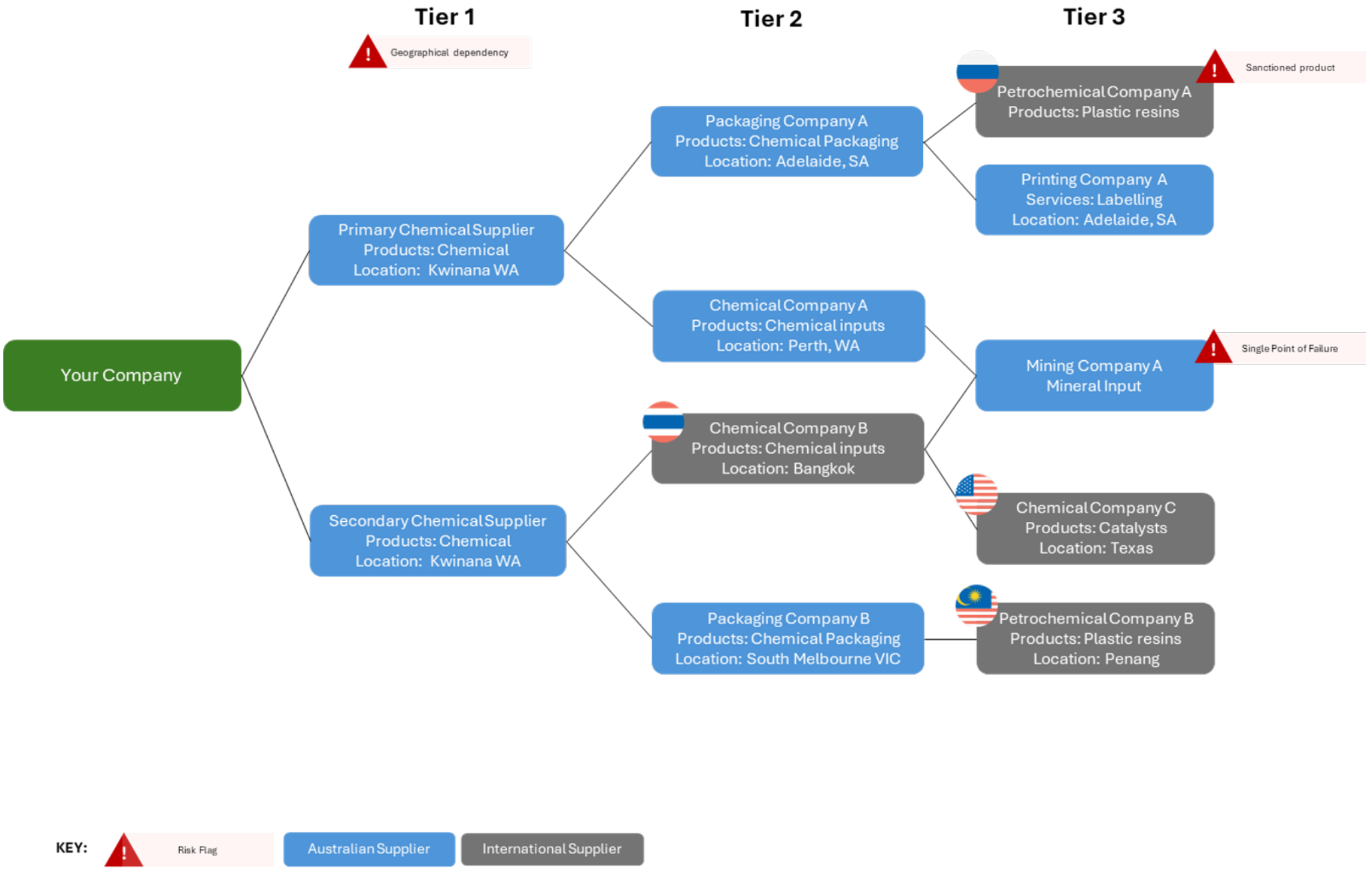
7.4.2.3 Illustrate the supply chain

Once you have sufficient information, develop a network diagram to visualise the supply chain. The diagram can take the form of a map, flowchart or other simple schematic, provided it clearly shows tiers and linkages between parties. Consider using a dedicated tool or software if the supply chain is complex or expected to change frequently. Ensure the diagram is updated as supplier information is validated over time.

Visualising the supply chain is an important step to help highlight potential vulnerabilities, such as single points of failure, geographic clustering and critical dependencies.

Figure 1 on the next page is an illustrative example of an option of how to visualise a lower complexity supply chain.

Figure 1: Illustrative example of a supply chain diagram.



7.4.3 Relying on third-party contractors to map your supply chain

When engaging third-party contractors to map your supply chain, it is essential to ensure the process is thorough, impartial, and aligns with your organisation's goals and risk profiles. There are several considerations your business should consider prior to engaging a contractor.

7.4.3.1 Internal buy in and support

The contractor will require significant buy in and support from internal teams to conduct supply chain mapping. To ensure the contractor receives sufficient internal support, ensure internal staff roles and responsibilities are clearly defined and key objectives are communicated with relevant teams.

Consider conducting preparatory work such as collating information on key suppliers to aid the contractor in initial steps of the mapping.

7.4.3.2 Establishing clear expectations

Contracts should clearly stipulate expectations for transparency, accuracy, and regular updates. Specify that contractors must collect information from all relevant tiers, not just direct suppliers, and require them to identify potential vulnerabilities or gaps in the chain. Mandate unbiased reporting, with mechanisms for verifying findings and addressing conflicts of interest, so the supply chain map reflects the true risk landscape.

Additionally, contracts should require contractors to establish mechanisms allowing for proactive updates to supply chain maps in response to supplier changes, incidents, or operational shifts.

7.4.3.3 Software

Consider utilising a contractor that has software that can be maintained, automated and accessed by necessary personnel within the organisation on an ongoing basis. This is particularly valuable where supply chains are complex and dynamic.

7.4.4 Identify supply chain vulnerabilities

A structured approach to identification and management of vulnerabilities will help ensure that mitigation actions are well-planned, transparent, accountable, and underpinned by robust evidence. At a high-level, undertake assessments to assess the:

- exposure and vulnerability by identifying whether a supply chain is prone to significant disruptions
- criticality by determining the scale of implications a disruption may have (both human and business impacts)
- residual risk by examining existing mitigations to prevent or manage supply chain disruptions.

7.4.4.1 Assess exposure and vulnerabilities

Once a supply chain has been mapped it should be assessed for points of exposure and vulnerability. Supply chains that are more exposed or vulnerable to threats and hazards tend to exhibit three broad characteristics.

Geographic clustering – when critical suppliers, sites or logistics routes are concentrated in the same region, localised disruptions (such as natural disasters, extreme weather, industrial action or geopolitical events) can have outsized impacts.

Limited flexibility – reliance on a single (or small number of) supplier(s), technologies or routes reduces the ability to switch quickly when disruptions occur.

Length – supply chains that cross multiple borders and jurisdictions can be more susceptible to transport delays, customs constraints, foreign regulatory change and geopolitical risk.

To assess exposure and vulnerability it is recommended to use indicators to measure the risk in a clear and repeatable way. *Table 2* below highlights some example indicators that can be used at each relevant tier (Tier 1, Tier 2 and n-tier where feasible). **Each organisation should set applicable ratings to define the thresholds as it applies to their business**.

Table 2: Example Indicators

Indicator	Description	Possible Measures	Example Rating
Single points of failure	Identify dependencies on single suppliers, sites or route dependencies that could cause a disproportionate disruption if they fail. E.g. multiple Tier 1 suppliers may rely on the same Tier 2 supplier to provide a critical part.	Number (or %) of critical inputs or services that have only one supplier/site/route at the relevant tier.	Low Risk = 0; Medium = 1-2; High = 3+ sole dependencies
Supplier concentration	Describes how dependent you are on a small number of suppliers for a given input, service, route or capability. Higher concentration typically increases vulnerability because disruption at one supplier (or one shared upstream dependency) can materially affect continuity.	Herfindahl–Hirschman Index (HHI)	Low concentration: HHI < 1,500; Moderate concentration: 1,500 ≤ HHI < 2,500; High concentration: HHI ≥ 2,500
		Spend or volume by supplier/contract	Low: all suppliers <40%; Moderate: 40-70% with one supplier; High >70% with one supplier
		Count of viable alternatives	High concentration = 0–1; Medium = 2–3; Low = 4+ alternatives
Market concentration	Measures the extent to which an input, product or service could be sourced from alternative suppliers.	Number of credible alternatives	High concentration = 0–1; Medium = 2–3; Low = 4+ alternatives
Import dependency	Assesses the extent to which a supply relies on overseas production rather than local production. Treat import dependency as higher where most volume or spend is sourced offshore and there are few viable domestic or in-region alternatives.	% of spend/volume sourced offshore per product	Low <20% offshore Moderate: 20 - 50% offshore; High >50% offshore
		Number of feasible domestic alternatives	High dependency = 0–1 domestic alternatives; Medium = 2–3; Low = 4+ alternatives

The measures above will help flag the types of vulnerabilities responsible entities and their supply chain may be exposed to. High supplier concentration and high geographic clustering often correlate with limited flexibility, while longer offshore supply chains can increase exposure to transport, regulatory and geopolitical risks.

The exposure and vulnerability matrix (*Figure 2*) can be used to integrate insights from quantitative data with qualitative judgements. It combines the scales of exposure to and frequency of disruptions to assess a supply chain's overall vulnerability.

On the left-hand side of the matrix, the exposure to disruption captures the availability of alternative sources of the product, how concentrated existing sources of supply are and whether the good can be substituted. Across the top of the matrix, the frequency of disruption to the supply chain is estimated by taking into account advice provided by subject matter experts.

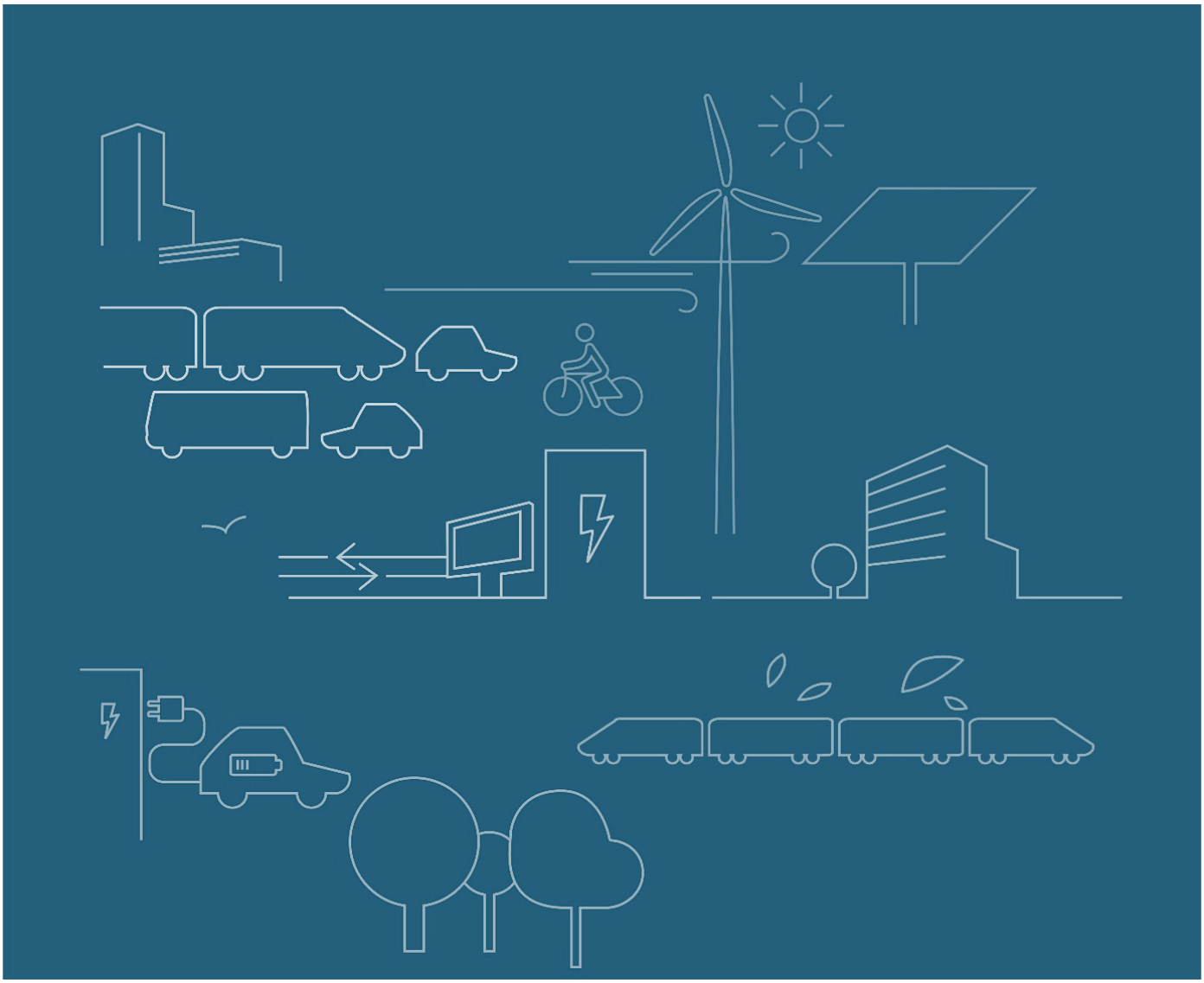


Figure 2: Exposure and vulnerability matrix

Exposure to disruption	Frequency of disruption				
	Extremely infrequent [Near-zero] chance to occur in the next 10 years	**Very infrequent [1 in 100] chance to occur in the next 10 years**	**Infrequent [1 in 10] chance to occur in the next 10 years**	**Frequent [1 in 5] chance to occur in the next 10 years**	**Very frequent [1 in 2] chance to occur in the next 10 years**
Critically exposed to disruption • dependent on one or few sources • no substitutes • no ability to develop alternative sources		Moderate Vulnerability	High Vulnerability	Severe Vulnerability	Severe Vulnerability
Highly exposed to disruption • highly concentrated supply • no or few viable substitutes • no ability to develop alternative sources	Low Vulnerability	Slight Vulnerability	Moderate Vulnerability	High Vulnerability	Severe Vulnerability
Moderately exposed to disruption • moderately concentrated supply • potential for substitutes • ability to eventually develop alternative sources	Low Vulnerability	Slight Vulnerability	Moderate Vulnerability	Moderate Vulnerability	High Vulnerability
Somewhat exposed to disruption • slightly concentrated supply • substitutes available • ability to rapidly develop alternative sources	Low Vulnerability	Slight Vulnerability	Slight Vulnerability	Slight Vulnerability	Moderate Vulnerability
No exposure to disruption • diversified supply • many substitutes available • easy to rapidly use alternative sources	Low Vulnerability	Low Vulnerability	Low Vulnerability	Low Vulnerability	Low Vulnerability

7.4.4.2 Assess criticality

After you identify vulnerabilities, assess if the affected supply chains are essential for the operation of the asset and fulfilling customer commitments. Having clear criteria for distinguishing between critical and non-critical supply chains helps you determine where disruption risk is and is not acceptable, and where additional controls or mitigations are warranted.

A criticality assessment should consider two complementary perspectives of business and human impact. For many organisations, particularly those delivering essential or safety-related services both lenses are relevant and should be assessed together.

Business impact typically includes financial impacts, cost impacts, and operational impacts. It also includes customer and market impacts (including reputational), compliance and legal exposure. It is important you define material impacts for your business (for example, by using internal thresholds for downtime, financial loss, safety, or breach severity) so criticality ratings are applied consistently. Where possible, align the matrix to your existing Business Continuity Plans (BCP) and risk frameworks.

Human impact considers the real-world effects of disruption on people who rely on your products or services, including customers and end users, your workforce, and the broader community. This is particularly important where you deliver essential services, operate in safety-critical environments, or support vulnerable cohorts. Human impact is typically higher where a good or service cannot be readily substituted and disruption could affect health, safety and wellbeing, interrupt access to essential services and basic needs, or create wider community impacts through flow-on disruption to essential organisations you support.

Consider *Tables 3* and *4* as examples of criticality matrices for human and business impact. As either the anticipated impact or the scale of disruption increases, the supply chain becomes more critical. The impact and scale thresholds should be tailored to your business context and reviewed periodically.

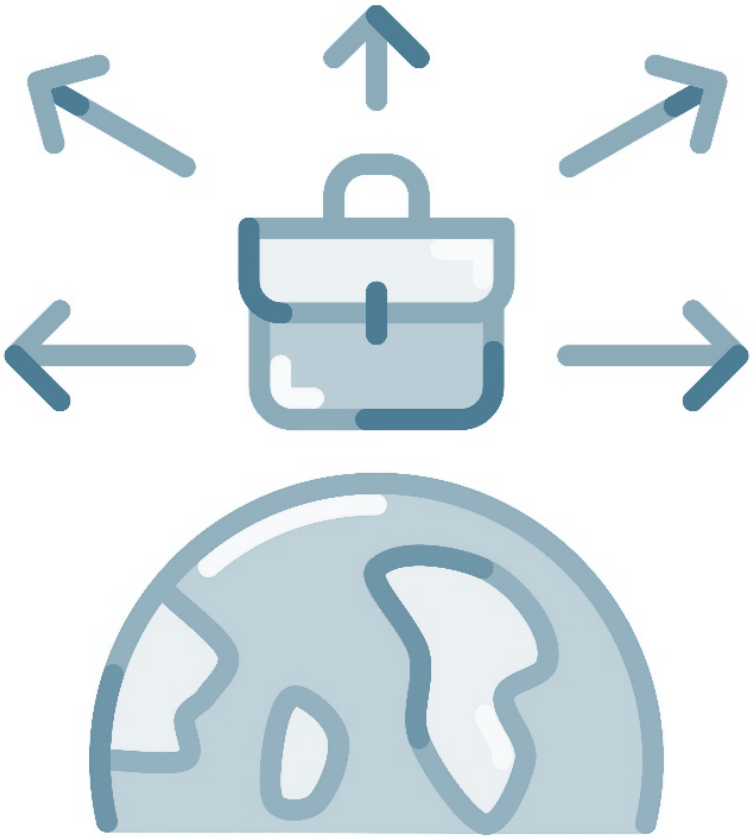


Table 3: Example business impact criticality matrix

Business impacts	Scale			
	Localised single team/site	**Multi-site several teams/sites**	**Enterprise wide most operations**	**Systemic enterprise and key customers/ partners**
Critical Sustained outage or severe non-performance; major legal/compliance breach; existential financial impact.	High	Severe	Catastrophic	Catastrophic
Major Extended disruption; significant customer impact; material financial loss; reportable incident likely.	Medium	High	Severe	Catastrophic
Moderate Short-term disruption; manageable workaround; moderate cost uplift; limited SLA breaches.	Low	Medium	High	Severe
Minor Minimal disruption; no material financial or compliance impact; low customer impact.	Low	Low	Medium	High

Table 4: **Example human impact criticality matrix**

Human impact	Scale				
	< 1,000 customers/end users impacted **Impact on a small cohort or single site/service area**	**1,000+ customers/end users impacted** **Concentrated impact on a cohort or region**	**10,000+ customers/end users impacted** **Concentrated impact across multiple service areas**	**100,000+ customers/end users impacted** **Large region or major service area impacted**	**1,000,000+ customers/end users impacted** **Widespread impact or cascading disruption across sectors**
Lives at risk Credible risk to life if the essential service is not available	Medium – High	Medium – High	Severe	Catastrophic	Catastrophic
Health and safety at risk essential services unavailable or rationed; increased safety risk or emergency response impacts	Low	Low	Medium – High	Severe	Catastrophic
Wellbeing at risk Disruption to basic needs, work and education; sustained loss of normal functioning	Nil	Low	Medium – High	Medium – High	Severe
Lifestyle and downstream customers at risk common services disrupted; reduced downstream economic activity; inconvenience to most users but safety not credibly affected	Nil	Low	Low	Low	Medium – High
Luxuries at risk non-essential amenities disrupted; minimal flow-on impacts	Nil	Nil	Nil	Nil	Nil

7.4.5 Residual risk

Following the assessment of vulnerabilities and criticality, existing mitigations should be considered and residual risk assessed.

Residual risk = inherent disruption risk − the effect of current controls and mitigations.

When assessing residual risk consider the effectiveness and coverage of the resilience measures already in place across the supply chain. Use the outcomes to decide whether the residual risk is within your organisation's risk appetite and impact tolerances, or whether additional treatment is required. Where residual risk remains above tolerance, ensure there is clear governance for escalation and formal risk acceptance by the appropriate accountable owner.

A practical way to structure this assessment is to consider the supply chain's capacity to:

- **Prevent** disruption where possible (reduce likelihood and exposure).
- **Cope** during disruption (maintain or degrade service safely within tolerances).
- **Adapt** as conditions change (switch suppliers, routes, materials, or operating modes).
- **Transform** over the longer term (change designs, processes, sourcing models, or technology to reduce dependency).

Figure 3 sets out example questions that can be used with subject matter experts to assess residual risk and identify gaps in resilience measures.

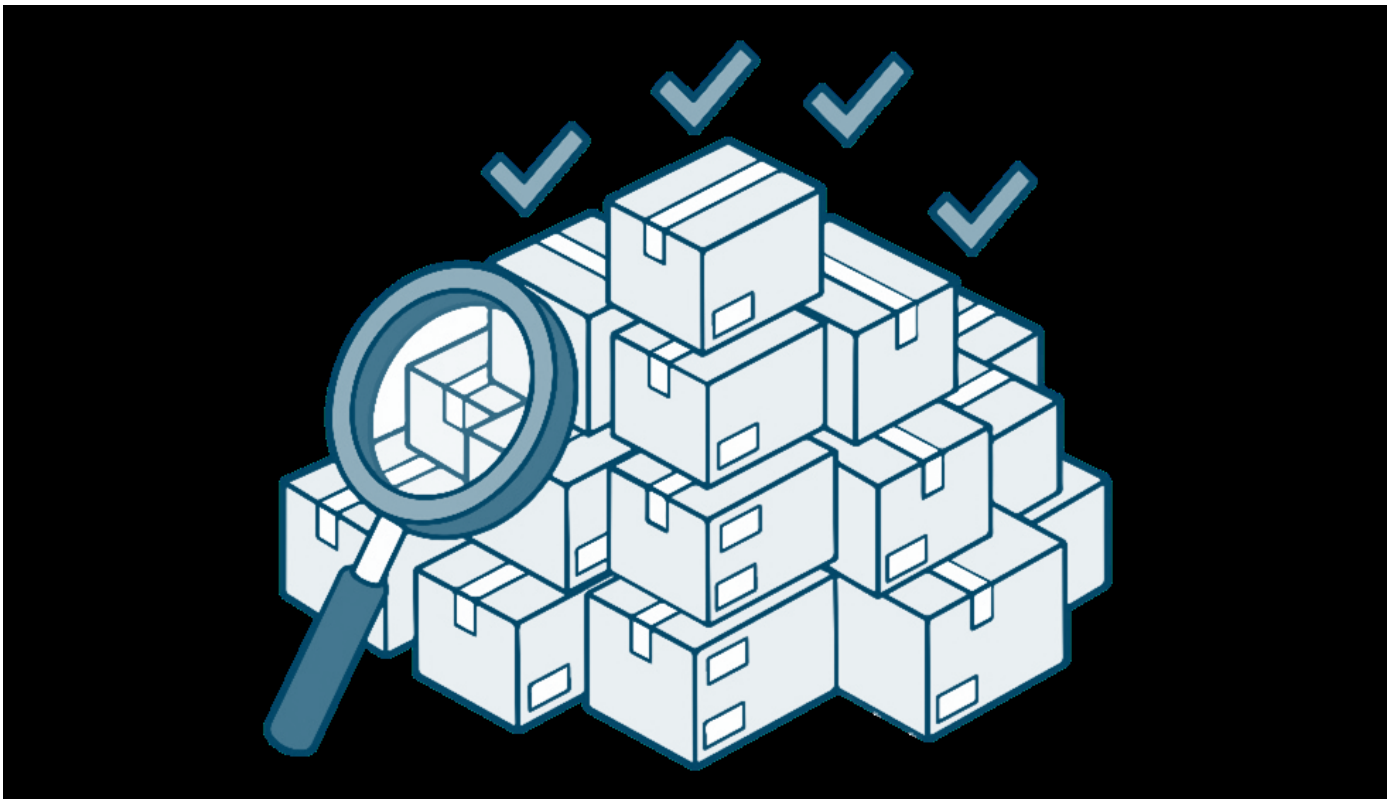


Figure 3: Dimensions of supply chain resilience and assessing residual risk



Capacity to prevent

Does the supply chain have capacity to address risks by managing the likelihood or level of exposure to potential disruption (e.g. through strong business to business links or backup supply arrangements)?

Have second-order vulnerabilities within the supply chain been identified and can they be managed?



Capacity to cope

How long could activities that deliver critical outcomes absorb a disruption (e.g. through rationing and stockpiles) before impacts become intolerable?



Capacity to adapt

Are there suitable alternative suppliers available in the market? If so, after how long could activities that deliver critical outcomes begin receiving these supplies?

Is there capacity within the existing supply chain to boost output and sustain crisis response efforts?

Are adaptation pathways robust enough to withstand extended periods of supply distress?

Do adaptive measures have long-term effects on recovery of opportunities for reward?



Capacity to transform

If there are no suitable alternative sources of supply, how long could either users or producers in a supply chain transform their processes to reduce dependence on disrupted products or suppliers?

Can aspects of the supply chain be de-risked through a permanent shift in its source? If so, what are the risks associated and can they be effectively managed (e.g. localisation of manufacturing etc.)?

Consider the answers holistically to determine whether gaps in resilience exist over the likely duration of a disruption, and to confirm the residual risk level once current mitigations are taken into account.

Identifying residual risk does not automatically mean further action is required. Some level of risk is inevitable and may be acceptable given the cost, feasibility and time required to mitigate it. The objective is to understand whether residual risk is within your organisation's risk appetite and impact tolerances, and to ensure any acceptance is explicit, owned, and reviewed.

It is important to assess the residual risk as an ongoing process as mitigations may evolve or change in effectiveness. Ensure a review mechanism is in place to reassess residual risk periodically or when key parameters change.

7.5 Illustrative case studies

This section provides two short, real-world case studies illustrating supply chain vulnerabilities that have arisen in practice and the types of responses that were used. These examples are illustrative only and are not intended to prescribe specific actions.

The case studies are:

- illustrative rather than prescriptive
- applicable across different business sizes and sectors
- designed to complement the mitigations above

Case study 1: Intravenous (IV) fluids supply disruption

Australia experienced shortages of intravenous (IV) fluids following disruptions affecting domestic manufacturing capacity and global supply chains. IV fluids are a critical hospital input with limited substitutability, meaning shortages had immediate impacts on clinical operations. In response, government and industry implemented a range of measures, including approving the temporary importation of substitute overseas-registered products and supporting expansion of domestic manufacturing capability.

These actions helped stabilise supply in the short term while reducing vulnerability to future disruptions through increased domestic capacity and diversification of supply. The experience illustrates the importance of diversification, substitution planning and the role of government-industry coordination where inputs are critical and substitutes are limited.

Case study 2: Pallet availability and logistics constraints

During periods of heightened demand and supply chain stress, shortages of pallets disrupted freight and retail supply chains, despite pallets being a relatively low-value input. Hoarding behaviour and limited interoperability between pallet pooling systems exacerbated the problem, creating bottlenecks across multiple sectors. Industry and government responded through increased information sharing, temporary coordination arrangements, and operational adjustments to improve pallet circulation and recovery.

The experience highlighted how non-critical inputs can become systemically important during disruption, and the role of coordination and behavioural responses in addressing supply chain vulnerabilities. The case highlights how visibility, coordination and behavioural responses can be as important as physical supply when managing system-wide disruptions.

7.6 Worked Example – CIRMP Entry

Field	Example Response
Hazard	Sub-standard or counterfeit component introduced through the supply chain causes equipment failure or degraded performance, disrupting the proper function of the CI asset.
Asset(s) / Site	Primary Operations Centre – Site A. The asset relies on specialist replacement components for operational equipment. Some components have long lead times and cannot be readily substituted during urgent maintenance.
Scenario	A replacement component is sourced through an approved supplier or distributor under time pressure during urgent maintenance. The component appears genuine but is sub-standard or counterfeit. After installation, the component fails or performs below specification, affecting the equipment and delaying restoration while a verified replacement is sourced.
Why this is material	The component supports equipment required for the proper function of the CI asset. Failure or degraded performance could disrupt operations and extend restoration beyond the maximum tolerable outage, particularly where verified replacement parts and specialist support are not immediately available.
Relevant impact mapping	**Integrity:** a compromised component undermines system integrity and may invalidate assurance about the condition or performance of the equipment. **Reliability:** sub-standard performance increases the likelihood of repeat failures and unreliable operation. **Availability:** equipment failure and delayed replacement may extend disruption to the asset's functions.
Evidence supporting likelihood	▪ Previous component failures, warranty claims and maintenance records, including failures shortly after installation. ▪ Manufacturer and supplier alerts about counterfeit or non-conforming components. ▪ Quality inspection, testing and assurance results for received components.
Key dependencies / interdependencies **(Include here the cascading impact that may result from the realisation of the hazards)**	▪ Approved suppliers, distributors and original equipment manufacturers. ▪ Limited stock or long lead times may extend the outage and affect dependent operations. ▪ Operational equipment that depends on the component and may be unavailable while the component is replaced.
Controls — Preparedness	▪ Identify high-criticality and long-lead-time components and record maximum tolerable outages. ▪ Establish escalation arrangements where standard approved sources cannot meet operational timeframes. ▪ Maintain verified spares or buffer stock for selected high-criticality components.
Controls — Prevent / minimise likelihood	▪ Purchase critical components from approved and verified suppliers or authorised distributors. ▪ Inspect and test critical components before installation, proportionate to their criticality and the sourcing circumstances. ▪ Monitor supplier performance, non-conformance reports and manufacturer alerts.
Controls — Impact mitigation	▪ Isolate and remove suspected components from service and quarantine related stock. ▪ Engage the manufacturer or specialist provider to verify the component and support restoration. ▪ Notify relevant internal stakeholders and update procurement controls following confirmed non-conformance.

Owners / status / timeframes	▪ Critical spares and inventory management — Maintenance Manager (In progress; Dec 2026). ▪ Supplier assurance and approved-source controls — Procurement Manager (Implemented; annual review). ▪ Urgent procurement procedure — Operations Manager (Implemented; next exercise Nov 2026).
Residual risk and acceptance	Residual risk assessed as medium due to long lead times for specialist components, reliance on external distributors and the difficulty of identifying sophisticated counterfeits through visual inspection alone. Accepted by the Risk Committee (Jun 2026), subject to completion of the critical-spares review and ongoing supplier assurance.
Review cadence / triggers	▪ component failure, suspected counterfeit or quality-related near miss ▪ an urgent or non-standard procurement ▪ a supplier, distributor or manufacturer alert ▪ a change in supplier, distribution pathway or component specification ▪ repeated non-conformance or warranty issues
Supporting material	▪ Critical component and spare-parts register ▪ Approved supplier and distributor list ▪ Certificates of conformity, inspection results and acceptance testing records ▪ Manufacturer or supplier alerts ▪ Urgent procurement procedure and approval records

Table of contents: Chapter 8

8.1 Obligations for managing physical security and natural hazards 124
8.2 Meeting the obligations in practice 126
8.2.1 Identify physical critical components of the CI asset 126
8.2.2 Minimise or eliminate a material risk, and mitigate a relevant impact 127
8.2.3 Respond to incidents where unauthorised access to a physical critical component occurs 127
8.2.4 Control access to physical critical components 128
8.2.5 Test arrangements to detect, delay, deter, respond to, and recover from unauthorised access 129
8.2.6 Centrally manage physical security and natural hazards 130
8.2.6.1 Location, ownership and nature of the site 130
8.2.6.2 Critical components of the CI asset 131
8.2.6.3 Areas holding business critical data or contain critical components 131
8.2.7 Outline and consider risk associated with other hazards which impact physical security 131
8.3 Best practice for identifying and mitigating risks 132
8.3.1 Material risk for consideration 132
8.3.2 Treating risk – mitigations and controls 133
8.3.2.1 Facility and security management 133
8.3.2.2 Surveillance and monitoring 133
8.3.2.3 Layered access controls 134
8.3.2.4 Early warning, monitoring and alerts for natural hazards 135
8.3.2.5 Preparedness, response and recovery 135
8.3.2.6 Site selection and land-use planning 135
8.3.2.7 Structural and building resilience 135
8.3.2.8 Environmental and landscape controls 136
8.3.2.9 Climate change resilience 136
8.4 Worked Example – CIRMP Entry 136

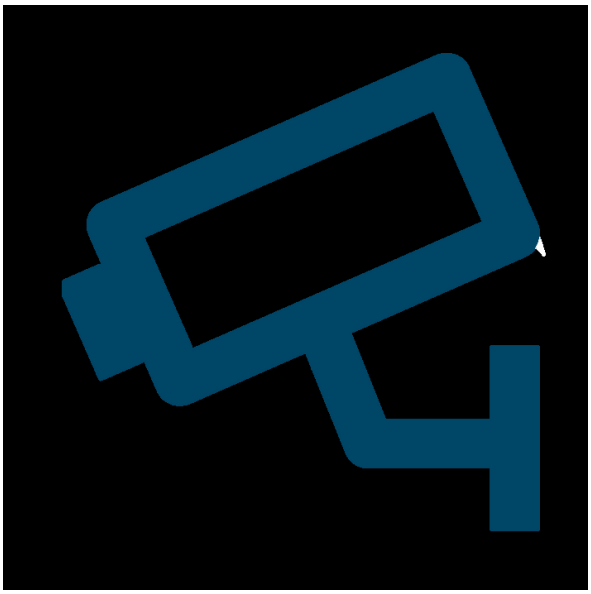
8. Physical security and natural hazards

Physical security and environmental controls play a critical role in the safe and continuous operation of CI assets. These assets are exposed to a range of physical security hazards, including unauthorised access, insider threats, theft, vandalism, and deliberate malicious acts, as well as natural hazards such as bushfires, floods, cyclones, severe storms, heatwaves, and other extreme weather events. Weaknesses in physical protections – such as inadequate access controls, poor site design, or insufficient active or passive monitoring – or a lack of preparedness for environmental conditions can expose critical components to damage, interference, or compromise.

A single threat arising from a physical security breach or natural hazard event can lead to serious consequences, including harm to personnel, damage to safety critical equipment, service outages, or reduced operational capability. For CI assets, these impacts may also cascade across interconnected systems, sectors, and communities, affecting public safety, economic stability, and the delivery of essential services. Managing physical security and natural hazard risks is therefore essential to maintaining the integrity, resilience, and continuity of Australia's critical infrastructure and to protecting national security and community wellbeing.

It is important to remember that physical security and natural hazards do not require a threat actor.





8.1 Obligations for managing physical security and natural hazards

The table below outlines the obligations in the CIRMP Rules in relation to physical security hazards and natural hazards. It outlines whether the obligations apply to responsible entities subject to the baseline and/or enhanced CIRMP requirements and/or TSRMP requirements.

The obligations are expanded on later in this chapter.

Physical security hazard and natural hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Responsible entities must establish and maintain a process or system in their CIRMP to identify the physical critical components of the CI asset.	S 11(1)(a)	s 11(1)(a)	S 15(1)(a)
Responsible entities must establish and maintain a process or system in their CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate a material risk and mitigate a relevant impact of: (i) a physical security hazard on a physical critical component; and (ii) a natural hazard on the CI asset.	s 11(1)(b)	s 11(1)(b)	s 15(1)(b)
Responsible entities must establish and maintain a process or system in their CIRMP to respond to incidents where unauthorised access to a physical critical component occur.	s 11(1)(c)	s 11(1)(c)	s 15(1)(c)
Responsible entities must establish and maintain a process or system in their CIRMP to control access to physical critical components, including restricting access to only those individuals who are critical workers or accompanied visitor.	s 11(1)(d)	s 11(1)(d)	s 15(1)(d)
Responsible entities must establish and maintain a process or system in their CIRMP to test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements.	s 11(1)(e)	s 11(1)(e)	s 15(1)(e)
Responsible entities must establish and maintain a process or system in their CIRMP to centrally manage physical security and natural hazards. For the purposes of this obligation the responsible entity must outline: (a) the location, ownership, and nature of the site upon which their asset is located; and (b) the critical components of the CI asset; and (c) areas within the asset that hold business critical data or contain critical components including critical systems.		s 11A(1)(a) s 11A(2)	

Responsible entities must establish and maintain a process or system in their CIRMP to – as far as it is reasonably practicable to do so – outline and consider the physical security consequences arising from the occurrence of all hazards, including cyber and information security hazards, credential compromise hazards, lateral movement hazards, other physical and natural hazards, personnel hazards, and supply chain hazards. For the purposes of this obligation the responsible entity must, as far as reasonably practicable, consider and outline the following: any physical access controls to the CI asset for workers, official visitors, and the public, including but not limited to: access controls for critical components and critical systems to restrict access to critical workers or accompanied visitors; maintaining surveillance and security alarm systems, such that critical components and critical systems are subject to continuous monitoring; specific protective security measures for business hours and out-of-hours; and other security measures that increase the ability to deter, detect, delay, respond to and recover from a breach in security for all critical components; and mitigation and response measures to be taken where a physical security incident or a physical security consequence has been detected.		s 11A(1)(b) s 11A(3)	

Timeframes for compliance are explained in Chapter 1 – **Introduction to the critical infrastructure risk management program (CIRMP)** at **1.5**

8.2 Meeting the obligations in practice

8.2.1 Identify physical critical components of the CI asset

CIRMP baseline – section 11(1)(a) of the CIRMP Rules

CIRMP enhanced – section 11(1)(a) of the CIRMP Rules

TSRMP – section 15(1)(a) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP are required to establish and maintain a process or system in their CIRMP to identify the physical critical components of the CI asset.

It is recommended that responsible entities maintain an understanding of all the critical components associated with their CI assets. Maintaining this understanding will assist them with complying with a range of obligations. Once responsible entities have identified all of their critical components, they can then determine which components are *physical*. This will support their compliance with this obligation.

The primary question responsible entities need to ask themselves as they assess whether a CI asset component is 'critical' is:

If this component was unable to function properly, would it prevent the CI asset from functioning or cause significant damage to the CI asset?

If the answer is yes, then the component is likely critical.

A **physical** critical component specifically refers only to those tangible or material parts of an asset where the absence of, damage to or compromise of the part would prevent the proper function of the asset or could cause significant damage to the asset.

If the CI asset is a **network of components** (such as a gas pipeline, telecommunications network, or water supply network) then the responsible entity should maintain a system for recording where components are located and should assess existing components as to their criticality. If the CI asset is a pipeline, it is likely that all components along a single pipeline are critical as if one were damaged, it may cause a stoppage in the pipeline. If the CI asset is a geographically dispersed network of components such as an electric power grid made up of generation plants,

transmission lines, and substations, then some of the components may not be critical, as the CI asset will still function if portions of the network fail.

If the CI asset is in a singular location, the responsible entity should assess what components of that asset are critical. For example, the control room of the CI asset may be critical because without it there is no other way to centrally manage the asset and deliver its critical function. It is unlikely that individual components such as security cameras, staff computers, software to manage administrative functions will be physical critical components.

Once the physical critical components have been identified it is recommended that the responsible entity maintain an up-to-date list or database of what the components are and where they are located.

It is recommended that the responsible entity maintain a system or process for assessing new components that are introduced to the CI asset environment to ensure the list is comprehensive and current.

8.2.2 Minimise or eliminate a material risk, and mitigate a relevant impact

CIRMP baseline – section 11(1)(b) of the CIRMP Rules

CIRMP enhanced – section 11(1)(b) of the CIRMP Rules

TSRMP – section 15(1)(b) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP are required to establish and maintain a process or system in their CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate a material risk and mitigate a relevant impact of a physical security hazard on a physical critical component or natural hazard on a CI asset.

This chapter of the guidance does not provide information on specified material risks under the CIRMP Rules. The material risks that are listed in section 6 and 6A of the CIRMP Rules are discussed in Chapter 2 – **All hazards**.

This chapter provides suggested material risks that are specific to physical security hazards and natural hazards. It also details potential mitigations. Refer to **8.3** of this chapter for this information.

8.2.3 Respond to incidents where unauthorised access to a physical critical component occurs

CIRMP baseline – section 11(1)(c) of the CIRMP Rules

CIRMP enhanced – section 11(1)(c) of the CIRMP Rules

TSRMP – section 15(1)(c) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP are required to establish and maintain a process or system in their CIRMP to respond to incidents where unauthorised access to a physical critical component occurs.

Mitigations such as layered access controls, surveillance and monitoring will assist responsible entities in responding to unauthorised access attempts. Appropriate processes to detect, delay, deter, and deny entry assist in preventing unauthorised access, but they also allow responsible entities more time for early response to prevent an incident.

When an incident occurs and a malicious actor has accessed a physical critical component there should be a documented, pre-established set of actions that the responsible entity will take to minimise impact on the physical critical component. It is recommended that this be practical, actionable, and have established roles and responsibilities.

When developing a response plan the responsible entity may consider:

- Containment and mitigation of impact to the asset and the essential service.
- Prevention of escalation (for example, sabotage or data compromise).
- Response capability and ability for instant and continuous monitoring to provide verification and triage.

Effective response plans clearly outline what constitutes unauthorised access (for example, entry to restricted areas without approval, tailgating into secure areas, or forced entry. This allows for appropriate detection of the unauthorised access. If it is not defined, it becomes more difficult to determine when unauthorised access has occurred.

The responsible entity should consider clearly outlining what the physical critical components are, where they are located, and relevant zones of access. To assist in identifying when unauthorised access has occurred the responsible entity should determine at what point of entry the access would exceed authorisation.

For example, if a physical critical component is in a locked room with five layers of access controls, at which layer would it be considered unauthorised access occurred. This will vary depending on the individual accessing the area and their authorisation level.

The responsible entity may consider outlining clear actions to respond to unauthorised access when it occurs. Clear prioritisation of action will allow for an effective response. The responsible entity may consider the below actions and whether they suit the environment and circumstances of the CI asset.

- Lock down access points.
- Increase or redirect security personnel or emergency services to the area.
- Disable compromised access credentials.
- Suspend operations of the component.
- Switch to fail safe or manual controls of the component.
- Isolate systems that may have been accessed.

These are suggested actions and is not an exhaustive list. Responsible entities should explore the full range of possible action, keeping in mind the nature of the CI asset and environment. This allows an appropriate assessment of what actions are reasonably practicable in the circumstances.

It is best practice to ensure it is clear who is responsible for the response in these circumstances. Having a clear incident leader and escalation methods allows for quick response and recovery.

8.2.4 Control access to physical critical components

CIRMP baseline – section 11(1)(d) of the CIRMP Rules

CIRMP enhanced – section 11(1)(d) of the CIRMP Rules

TSRMP – section 15(1)(d) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP are required to establish and maintain a process or system in their CIRMP to control access to physical critical components, including restricting access to only those individuals who are critical workers or accompanied visitors.

To comply with this obligation responsible entities must have identified critical workers and maintain procedures to ensure visitors remain accompanied when accessing the asset. For guidance on identifying critical workers, as well as best practice visitor procedures see **6.2.1** and **6.3.2.8** of Chapter 6 – **Personnel hazards**

Controlling access to physical critical components should include layered access control, surveillance, and monitoring. Details on controls to consider are provided at **8.3.2** of this chapter.

8.2.5 Test arrangements to detect, delay, deter, respond to, and recover from unauthorised access

CIRMP baseline – section 11(1)(e) of the CIRMP Rules

CIRMP enhanced – section 11(1)(e) of the CIRMP Rules

TSRMP – section 15(1)(e) of the TSRMP Rules

Responsible entities for CI assets are required to test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in arrangements.

- test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in arrangements (for responsible entities subject to the baseline or enhanced CIRMP).
- test the **extent** to which security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in arrangements (for responsible entities subject to the TSRMP).

Responsible entities should consider all hazards and their potential impact on physical security and access. For example, a cyber incident could result in doors disarming and enabling access to critical components. Responsible entities subject to the enhanced CIRMP have obligations to consider physical security consequences resulting from other hazards – see **8.2.7** for more detail.

Detect	Detection of unauthorised access starts with recorded, real time surveillance and monitoring. To allow for early detection, and provide more time for deterrence, it is best practice to have surveillance at entry points to a facility, rather than just on the critical components. Surveillance and CCTV that is not regularly monitored does not allow for timely detection. Consider CCTV capability and whether it allows for instant detection. Detection must occur at the earliest opportunity and, where possible, should be combined with hardened perimeters to create the delay and instigate the appropriate response
Delay	As with detection, delaying starts at the external areas of the facility. Consider ensuring critical components have multiple layers of access zoning leading to the component. If possible, they should be located at the deepest point within the facility to slow approach from malicious actors. Physical deterrents may also assist in delaying a malicious actor, for example terrain or landscaping features, or fencing will slow a malicious actor's approach
Deter	Deterrence refers to discouraging or preventing someone from attempting to access a facility or critical components. Deterrence can include dense vegetation (such as hedges, mountains, or water), security signage indicating constant monitoring, a lack of visible high value assets, or high security fencing.
Respond	A predetermined response plan ensures action can be taken quickly and effectively. Early detection will allow for early response. It is not effective to wait until an incident has occurred to respond. By detecting, deterring, and delaying there will be more time and ability to respond.
Recover	Recovery from an incident will vary widely depending on the assets and component affected. Recovering from an incident includes getting the system or component up and running again, but it also includes re-establishing the integrity, safety and reliability of the component or asset. When establishing a process for recovery consider whether the unauthorised access has ceased, the affected area is secure and controlled, and safety risks have been managed. Recovery requires testing of the component as well as inspection. In some cases, it may be necessary to stage restoration of services to ensure systems are running as appropriate.

Responsible entities must have a system for testing these arrangements and ensuring they are effective. Consider running exercises or penetration tests to determine whether systems prevent unauthorised access. These arrangements should be reviewed and tested regularly. Establishing a review period and triggers for review will ensure security arrangements are robust and meet baseline obligations.

Triggers for review could include:

- An incident has occurred.
- The threat landscape has changed and new risks are detected.
- The security system has changed.
- Operational or business changes.

It is best practice to appropriately document when a review has taken place and what the result of the review was. We encourage responsible entities to share insights on the outcome of reviews with internal and external stakeholders to build a shared understanding and responsibility for security.

8.2.6 Centrally manage physical security and natural hazards

Best practice for all responsible entities to consider

CIRMP enhanced – section 11A(1)(a) and 11A(2) of the CIRMP Rules

Responsible entities for CI assets that are subject to the enhanced CIRMP are required to establish and maintain a process or system in their CIRMP to centrally manage physical security and natural hazards.

For this purpose, the CIRMP must outline:

- The location, ownership, and nature of the site upon which the CI asset is located.
- The critical components of the CI asset.
- Areas within the asset that hold business critical data or contain critical components including critical systems

Responsible entities may rely on existing documentation to support this obligation. It requires the responsible entity to have a central program for management of physical security and natural hazards.

8.2.6.1 Location, ownership and nature of the site

Responsible entities must outline in their CIRMP the location, ownership, and nature of the site upon which the CI asset is located. If the CI asset is geographically dispersed, this will include all the areas on which the CI asset is located.

The ownership of the CI asset may include the owner of the asset itself or the land that the asset is located on. If the land is leased or co-owned then it is recommended that this information be recorded and centrally managed.

The nature of the site may refer to a range of factors. It may encompass any relevant physical, geographic, regulatory or environmental features that may influence the management of the CI asset. Responsible entities are encouraged to consider what features the site possesses and how that impacts the CI asset in practice. These features may include:

- Whether the CI asset is in an industrial, commercial or residential area.
- Whether the CI asset or its components are located remotely, offshore or onshore.
- The proximity of the CI asset to other CI assets or supporting services (for example, is it near to maintenance providers or emergency services).
- Any access arrangements or restrictions.
- Whether the CI asset is located in a shared facility or on a dedicated site.
- Any environmental conditions that may impact the operation or maintenance of the CI asset.
- Any other physical, geographic, regulatory or environmental features that could impact or influence the management of the asset.

As a reporting entity for a CI asset, the responsible entity will also be subject to the obligation to give information and notify of events in relation to their CI asset for the Register of CI assets, which is in Part 2 of the SOCI Act. This obligation requires the responsible entity to provide operational information, which includes the location of the asset and may include ownership information – for information on this see **Registering a Critical Infrastructure Asset.** Responsible entities are advised to consider managing these obligations together.

8.2.6.2 Critical components of the CI asset

Responsible entities are required to identify physical critical components (see **8.2.1** in this chapter), and responsible entities subject to the enhanced CIRMP are required to identify critical systems for lateral movement hazards (see **5.2.1** of Chapter 5 – **Lateral movement hazards**). Having a thorough understanding of all critical components of a CI asset will assist in appropriately managing risks to the CI asset and ensuring compliance with SOCI obligations. Having these components centrally managed allows responsible entities to maintain an understanding of where these components are and how they interact with other components. It also allows responsible entities to assess how the environment may affect the components or what cascading impacts could occur.

Responsible entities must record all critical components associated with the CI asset and regularly review and update these records.

8.2.6.3 Areas holding business critical data or contain critical components

Understanding where business critical data ands critical components are located, as well as how they are protected, will support the effective management of hazards and the potential consequences arising from disruption.

Areas holding business critical data may include physical records, server rooms, data centres, control rooms, operational technology environments, communications facilities, backup storage locations, or other areas where business critical information is maintained. If business critical data is stored in a third-party data centre, this should also be recorded appropriately.

Responsible entities should consider all critical components (including critical systems) when recording the areas in which they are located. Critical components may be co-located or located separately from the CI asset – such arrangements should be accurately and appropriately recorded.

Responsible entities should consider recording and centrally managing information such as:

- The location of areas holding business critical data or containing critical components.
- The purpose and function of those areas.
- The critical components or systems located within each area.
- Any physical security measures and access controls that protect the area.
- Dependencies between these areas and other parts of the CI asset.
- Environmental or natural hazard considerations relevant to the area.
- Any shared occupancy, third-party access arrangements, or outsourced management arrangements associated with the area.

Responsible entities are encouraged to regularly review and update records relating to these areas to ensure they remain accurate and reflect any changes to the CI asset.

8.2.7 Outline and consider risk associated with other hazards which impact physical security

Best practice for all responsible entities to consider

CIRMP enhanced – sections 11A(b) and 11A(3) of the CIRMP Rules

Responsible entities for CI assets subject to the enhanced CIRMP are required to establish and maintain a process or system in their CIRMP to – as far as it is reasonably practicable to do so – outline and consider the physical security consequences arising from the occurrence of all hazards, including cyber and information security hazards, credential compromise hazards, lateral movement hazards, other physical and natural hazards, personnel hazards and supply chain hazards.

The CIRMP Rules detail requirements for this obligation. Responsible entities must – as far as it is reasonably practicable – consider and outline:

- any physical access controls to the CI asset for workers, official visitors, and the public, including but not limited to:
  - access controls for critical components and critical systems to restrict access to critical workers or accompanied visitors;
  - maintaining surveillance and security alarm systems, such that critical components and critical systems are subject to continuous monitoring;
  - specific protective security measures for business hours and out-of-hours; and
- other security measures that increase the ability to deter, detect, delay, respond to and recover from a breach in security for all critical components; and
- mitigation and response measures to be taken where a physical security incident or a physical security consequence has been detected.

In **8.3.2** of this chapter there are suggested mitigations that may go to addressing the above points.

This obligation recognises that physical security incidents often do not occur in isolation and may originate from other hazard domains. In many cases a non-physical hazard can weaken security controls, reduce visibility of incidents, or prevent access controls from functioning as intended. It is recommended that responsible entities integrate this obligation into their consideration of other hazard vectors. For example, if the responsible entity is considering their supply chain material risks, they should also simultaneously consider the potential physical security consequences arising from the supply chain material risk.

It is recommended that responsible entities consider how the realisation of a hazard could affect their ability to detect, deter, delay, respond to, or recover from a physical security incident. Consideration should also be given to whether the hazard could:

- Disable or degrade physical access control systems.
- Reduce monitoring or surveillance capability.
- Create opportunities for unauthorised access to facilities or critical components.
- Prevent workers from accessing or securing sites.
- Increase reliance on manual processes or temporary workarounds.
- Result in the loss of accountability for personnel, visitors, equipment or credentials.
- Create cascading impacts that affect the physical operation, safety or security of the CI asset.

Responsible entities should also consider compound and cascading events. For example, a severe weather event may result in a prolonged power outage, which subsequently affects surveillance systems, electronic access controls and communications. Similarly, a cyber incident may coincide with a physical security event, reducing situational awareness and limiting the responsible entity's ability to respond. Considering these interconnected impacts will support a more comprehensive understanding of risk and improve preparedness, response and recovery arrangements.

8.3 Best practice for identifying and mitigating risks

This section provides guidance on best practice mitigations for risks associated with physical security hazards and natural hazards. Responsible entities should consider whether these mitigations will assist them in meeting their obligation to minimise or eliminate material risks or mitigate against relevant impacts (section 11(1)(b) of the CIRMP Rules and section 15(1)(b) of the TSRMP Rules). The guidance does not comprehensively cover all possible mitigation or risks. The responsible entity must consider additional mitigations as required to address all potential material risks to the CI asset.

8.3.1 Material risk for consideration

Responsible entities must mitigate against the specified material risks in the CIRMP Rules, however they should also consider other possible material risks.

Below are some suggested material risks for consideration. There may be other material risks that are not included in this guidance. It is the responsibility of the responsible entity to identify, eliminate, and minimise these material risks.

Risk Category	Description
Unauthorised access	Facilities may be targeted for ideological, strategic, or financial reasons. Trusted insiders may also present risk when they access areas without authorisation. Poorly maintained physical barriers exacerbate this risk.
Crime or deliberate physical crime	Includes terrorism, sabotage, espionage, insider threats, theft, and vandalism. Examples include damage to transformers, fibre cables, pipelines, or server racks; theft of copper, communications equipment, or hazardous materials and vehicle ramming.
Ageing or faulty infrastructure	Physical infrastructure failure, particularly where there are single points of failure, ageing assets, or inadequate perimeter protections. Co-located systems and insufficient physical separation between critical components can result in cascading failures.
Third-party and supply chain risks	Contractors, vendors, and service providers often require physical access to sensitive sites. Poorly managed third-party access introduces significant vulnerabilities. Physical disruptions to supply chains can delay critical materials and spare parts.
Environmental and natural hazards	Extreme weather events (floods, bushfires, cyclones, heatwaves) can damage assets, restrict access, and disrupt operations. Climate change is amplifying the frequency and severity of these natural hazards. Physical security planning must account for resilience, redundancy, and safe access during natural hazard events.

8.3.2 Treating risk – mitigations and controls

When developing this guidance, the *Australian Government Protective Security Policy Framework – Release 2025* (PSPF) was considered, and components of the PSPF have been integrated as best practice. The PSPF sets the Australian Government's minimum protective security standards for government entities. Whilst the PSPF applies to Australian Government entities, responsible entities may consider whether the advice within the PSPF could be adapted for their own purposes.

8.3.2.1 Facility and security management

It is best practice for all responsible entities to, at a minimum, have an established maintenance and review program for all parts of their security measures and systems. Responsible entities should consider centrally managing this program.

For example:

- There is a perimeter fence surrounding the CI asset. It should be regularly inspected to ensure it remains in good condition and that the surroundings do not render the fencing void (for example, no trees overhanging the fence or objects stacked against the fence).
- There is CCTV monitoring the perimeter. This system should be regularly checked to ensure all cameras are functioning, nothing is blocking their field of view, and their software is up to date.

Having a clear understanding of each part of the security systems assists responsible entities ensure there are appropriately established procedures to maintain and regular reviews these systems.

8.3.2.2 Surveillance and monitoring

Surveillance and detection controls enable early identification and response to security incidents. CCTV systems, intrusion alarms, motion sensors and duress alarms should be strategically positioned and actively monitored to deter criminal activity, trusted insider risk, support investigations and improve staff safety in higher-risk environments.

It is important to pair surveillance and monitoring controls with both perimeter access controls and response procedures. Perimeter controls will slow the entrance of a malicious actor, enabling the responsible entity more time to act to prevent unauthorised access or interference. A robust response procedure also allows the responsible entity to act quickly and coordinate defensive response.

8.3.2.3 Layered access controls

Layered access controls are considered best practice to control access to physical critical components. Implementation of layered access controls commonly involves having varying levels of security zones. This prevents unauthorised access to critical components and can assist in slowing malicious actors from gaining access to these components.

Layered access controls start at the initial perimeter of the asset and progresses through the facility with increasing levels of controls to prevent unauthorised access.

Perimeter controls

The perimeter controls are the first layer of defence against unauthorised access. These controls act as a deterrent and may slow the movement of malicious actors when they persist through barriers.

Consider having a range of deterrents, preventative measures, and detection measures.

Deterrent	Deterrents are often visual cues that may discourage unmotivated actors from entering the property. This can include: • bright lights to heighten visibility • signs indicating CCTV monitoring • difficult to traverse terrain.
Prevention	Prevention refers to things that will prevent or slow a malicious actor from gaining unauthorised access to the property. This can include: • Fencing • Locked doors • Vehicle mitigation barriers
Detection	Detection refers to processes that will assist the responsible entity in early detection of an attempt at unauthorised access. This can include: • CCTV systems with motion/thermal detection • Alarm systems • Security guards and patrols

Regularly inspecting and maintaining perimeter security controls ensures strong and resilient defence.

Facility hardening

Facility hardening refers to the deliberate strengthening of workplaces, infrastructure and physical systems to reduce vulnerability to security threats, limit damage during an incident, and protect occupants and critical assets. Unlike general security controls, hardening focuses on making a facility inherently more resistant to forced entry, attack, sabotage, or aggressive behaviour. Examples of controls may include steel doors, window grills, or blocker plates.

Internal access controls

Internal access controls will prevent malicious actors who have breached earlier defences and trusted insider threat actors from accessing critical components or sensitive information. Best practice controls for unauthorised access to critical components involves multiple layers of internal access controls. Responsible entities will likely have workers with various level of security clearance, and as such, the internal access controls should prevent those with lower clearances from accessing critical components.

Internal access controls may include:

- electronic systems such as key cards, PINs, mobile credentials, or biometrics
- zoned access
- lockable storage
- visitor management processes – see **6.3.2.8** of Chapter 6 - **Personnel hazards**
- timely removal of access for transferring or departing staff – see **6.3.2.5** of Chapter 6 - **Personnel hazards**

These measures reduce the risk of theft, sabotage, data loss and operational disruption, particularly for systems essential to service delivery.

8.3.2.4 Early warning, monitoring and alerts for natural hazards

Early warning and monitoring systems enable organisations to act before hazards escalate. Access to official alerts, local monitoring data and clearly defined internal triggers supports timely decision-making, activation of response plans and implementation of protective measures.

After early warning or alerts are received, responsible entities should be prepared to activate their response and recover plans.

8.3.2.5 Preparedness, response and recovery

Responsible entities should be prepared for incidents or emergencies and have response and recovery procedures in place.

Preparedness for physical security incidents includes documented response procedures, clearly defined roles and coordination with emergency services. Post-incident reviews, staff support mechanisms and lessons learned processes help organisations recover effectively and reduce the likelihood and impact of future incidents.

Emergency preparedness ensures worker safety during natural hazard events. Documented emergency plans, clear evacuation or shelter-in-place procedures, defined roles and regular exercises improve coordination, reduce confusion and support effective responses under pressure.

Critical infrastructure and essential services response and recovery plans should be designed to ensure continuity during natural hazard and physical security events.

Preparedness should be treated as a living practice, not a document-and-forget activity.

8.3.2.6 Site selection and land-use planning

Where possible, organisations should consider site selection and land-use when making decisions for new assets or critical components.

The area in which a component or asset is established can introduce new risks or act as mitigations against risk. For example, an area that is prone to high-risk weather events will create a natural hazard for the component or asset. Conversely, selecting a site that has natural defence, such as dense scrub, may assist in mitigating risks of unauthorised access.

Consider below some factors that may impact site selection:

- High risk areas such as floodplains, bushfire-prone zones, or unstable land.
- Zoning controls.
- Areas that may result in protests from issue motivated groups.
- Convenience of location for unauthorised access from unmotivated parties.

If a site is selected despite risks, the responsible entity must consider what mitigations must be implemented to reduce the risk of these events. Appropriate selection of sites can assist in improving long-term risk management and prioritisation of controls for new and existing facilities.

Additionally, responsible entities should consider whether the site selected is appropriate for the use of the component or CI asset, and whether the location is appropriate. Some assets may benefit from being in densely populated areas, while others may benefit from being remotely located. It is important to consider what best suits the asset and mitigate against the risks presented by the area selected.

8.3.2.7 Structural and building resilience

CI assets should be designed or retrofitted to withstand foreseeable natural hazards through resilient construction and materials. Measures such as flood-resistant finishes, bushfire-resistant design, cyclone-rated fixings, seismic strengthening and adequate roof drainage reduce damage, protect occupants and speed up post-event recovery.

Additionally, responsible entities should consider whether the building has appropriate structural defence. For example, responsible entities should consider whether delicate critical componentry should be in a building with floor to ceiling windows. If this occurred, the responsible entity would be required to consider appropriate mitigations to prevent unauthorised entry through these windows or should ensure that the componentry has layered defence in the xevent of a forced entry.

8.3.2.8 Environmental and landscape controls

Management of the surrounding environment plays an important role in reducing hazard exposure. Vegetation management, fuel load reduction, effective drainage, erosion control and securing loose materials help limit the intensity and spread of hazards such as bushfire, flooding and storm damage.

8.3.2.9 Climate change resilience

Climate change is increasing the frequency, severity and duration of many natural hazards, including floods, bushfires, cyclones, severe storms, coastal inundation and extreme heat. Responsible entities should consider both current and future climate-related risks when assessing the resilience of CI assets and critical components. Climate resilience should be integrated throughout the asset lifecycle, including planning, design, construction, operation, maintenance, renewal and decommissioning activities. Responsible entities should seek to ensure assets can anticipate and recover from climate-related disruptions while maintaining critical functions and essential service delivery.

Responsible entities are encouraged to consider:

- Incorporating climate projections into risk assessments and planning.
- Undertaking periodic reviews of hazard exposure and climate vulnerability.
- Designing, upgrading or retrofitting assets to withstand foreseeable future climate conditions.
- Introducing redundancy, backup systems and alternative operating arrangements for climate-sensitive critical components.
- Considering climate-related risks when selecting sites for new infrastructure or major asset replacements.
- Assessing cross-sector dependencies, including reliance on energy, communications, transport, water and supply chain networks during climate-related disruptions.

Testing response and recovery plans against prolonged or concurrent climate-driven hazard events.

8.4 Worked Example – CIRMP Entry

Below is an example of a natural hazard, the assessment a responsible entity may record to determine whether the hazard is a material risk and the controls in place to manage the risk and the impact of the eventuation of the risk. This example is a suggestion, and there is no requirement for responsible entities to record their assessments in this way.

Field	Example Response
Hazard	Flooding (riverine / flash flooding).
Asset(s) / Site	Primary Operations Centre – **Site A** (includes control room, comms racks).
Scenario	A 1-in-100 year rainfall event causes site access to be cut and water ingress to the ground-floor comms room for 48 – 72 hours.
Why this is material	The scenario could cause disruption to essential monitoring/control capability and communications for an unmanageable period, with potential safety impacts for dependent field operations.
Relevant impact mapping	**Availability:** loss of monitoring/control and communications capability **Reliability:** degraded ability to support dependent field operations.
Evidence supporting likelihood	• Council flood overlays • Historical incidents (2011/2022 events) • Insurer site assessment • Drainage capacity study
Key dependencies / interdependencies (Include here the cascading impact that may result from the realisation of the hazards)	Dependent on the availability of Site A: • Corporate network • Operations of network • Remote access to critical componentry

Controls — Preparedness	• Flood response checklist (roles, contacts, call-out tree) • Lessons learned from 2022 event • Pre-arranged restoration contractor and parts kit on site
Controls — Prevent / minimise likelihood	• Drainage upgrades completed (2025) and quarterly maintenance schedule • Raise thresholds and seal penetrations to comms room • Relocate critical comms equipment above flood line (planned)
Controls — Impact mitigation	• Failover to Secondary Operations Centre – **Site B within 2 hours** • Manual operating procedures for priority functions during failover
Owners / status / timeframes	• Drainage maintenance — Facilities/Ops — Implemented; ongoing quarterly • Sealing thresholds/penetrations — Facilities — Scheduled • Comms relocation — IT/OT Ops — Planned; FY27 milestone • Failover testing — Operations/BCP Lead — Scheduled
Residual risk and acceptance	Residual risk assessed as medium due to remaining exposure to access disruption during extreme events. Risk acceptance approved by the Risk Committee; additional mitigation (equipment relocation) funded for FY26.
Review cadence / triggers	Formal review annually as part of CIRMP review. Trigger review after: • Any flood incident / near miss • Material site changes • Updated flood mapping
Supporting material	• Flood overlay map • Drainage study • Insurance risk report • Maintenance logs • Photos of upgrades • Project plan for relocation • BCP/failover test results • Exercise record and after-action review • Risk acceptance record • Previous CIRMP annual attestations

Table of contents: Chapter 9

9.1 Obligations for maintaining the CIRMP 140
9.2 Meeting the obligations in practice 141
9.2.1 Establish and maintain a process or system to review the CIRMP to ensure compliance with 30AE of the SOCI Act 141
9.2.2 Regular reviewing of the CIRMP 141
9.2.2.1 What is a regular basis 141
9.2.2.2 Ensuring the CIRMP is up to date 141
9.2.3 What are reasonable steps? 141
9.2.4 What to consider when reviewing the CIRMP 141
9.2.5 Trigger based reviewing of the CIRMP 142
9.2.5.1 Reviewing the whole CIRMP 142
9.2.5.2 Reviewing a component of the CIRMP 142
9.2.6 Establish and maintain a process or system to keep the CIRMP current to ensure compliance with 30AF of the SOCI Act 143
9.2.7 A responsible entity must have regard to certain matters in deciding to whether to adopt or vary the CIRMP 143
9.3 Annual reporting requirements 145
9.3.1 What information must be included? 146
9.3.2 Board approval 146
9.3.3 Timeframes for submission 146

9. Maintaining the CIRMP and annual reporting requirements

Responsible entities are required to maintain their CIRMP. This involves ensuring there are processes in place to manage the adoption, variation, review of the CIRMP. A CIRMP should not be a static document. It should reflect the changing threat environment, the operation of the asset, lessons learned, and updates to legislative or regulatory requirements.

An effective CIRMP embeds risk management as an active process that is undertaken organisation wide. It should be current and relevant to the CI asset, and internal compliance with the CIRMP should be a priority.

Responsible entities are also required to submit an annual report to the relevant commonwealth regulator. The annual report must be approved by the board, council or other governing body. This provides the governing body appropriate oversight of the risks facing their CI assets. It also allows them to ensure resources are appropriately allocated to support security and reliability of their CI asset and to comply with SOCI obligations. The annual report also provides the opportunity for the regulator to determine if the responsible entity requires assistance or guidance in updating their CIRMP and allows the Department of Home Affairs to build a collective picture of the nature of threats impacting CI assets across all sectors.



9.1 Obligations for maintaining the CIRMP

The table below outlines the obligations in the SOCI Act and the CIRMP in relation to maintaining the CIRMP. It outlines whether the obligations apply to responsible entities subject to the baseline and/or enhanced CIRMP requirements and/or TSRMP requirements. The obligations are expanded on later in this chapter.

Maintaining the CIRMP and annual reporting obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
The responsible entity must establish and maintain a process or system in the entity's CIRMP to review the CIRMP to ensure compliance with section 30AE of the Act.	s 7(1)(d)	s 7(1)(d)	s 9(d)
The responsible entity must establish and maintain a process or system in the entity's CIRMP to keep the CIRMP current to ensure it complies with section 30AF of the Act	s 7(1)(e)	s 7(1)(e)	s 9(e)
	SOCI Act		
A responsible entity must have regard to certain matters in deciding whether to adopt a CIRMP, and when reviewing or varying their CIRMP.	30AKA	30AKA	30AKA
A responsible entity must give an annual report relating to its critical infrastructure risk management program. If the entity has a board, council or other governing body, the annual report must be approved by the board, council or other governing body.	30AG	30AG	30AG
A responsible entity for a critical infrastructure asset that is exempt from Part 2A of the SOCI Act (pursuant to sections 30AB(4)-(6) of the SOCI Act) must give an annual report in accordance with Part 2AA of the Act.	30AQ	30AQ	30AQ



9.2 Meeting the obligations in practice

9.2.1 Establish and maintain a process or system to review the CIRMP to ensure compliance with 30AE of the SOCI Act

CIRMP baseline – section 7(1)(d) of the CIRMP Rules

CIRMP enhanced – section 7(1)(d) of the CIRMP Rules

TSRMP – section 9(d) of the TSRMP Rules

9.2.2 Regular reviewing of the CIRMP

Responsible entities that have adopted a CIRMP must also review the program on a **regular basis** (section 30AE of the SOCI Act). In undertaking this review, responsible entities must establish and maintain a process or system in the CIRMP to review the CIRMP on a regular basis (section 7(1)(d) of the CIRMP Rules and section 9(d) of the TSRMP Rules).

Responsible entities will likely need to review some parts of their CIRMP more often than other parts. Events may trigger a review of one hazard vector or material risk but will not require a review of the entire CIRMP. Responsible entities may undertake these partial reviews, however they must also undertake a collective review of the whole program on a regular basis.

When undertaking a review of the CIRMP, responsible entities must consider specified information as set out in the CIRMP Rules, or TSRMP Rules where applicable. See **9.2.4** in this chapter for the specified information. This ensures that the CIRMP is appropriate, effective, and adequately address the risks.

When undertaking a comprehensive review of the CIRMP, responsible entities must consider a broad range of matters across all hazard vectors. The matters the responsible entity must consider vary between the CIRMP and TSRMP. For information on the TSRMP see the **Guidance for Responsible Entities for Critical Telecommunications Assets**.

9.2.2.1 What is a regular basis

Regular basis is explained in the **glossary**.

It is expected that responsible entities will undertake regular scheduled reviews, as well as triggered based reviews. It is best practice to undertake a review of the entire CIRMP **every 24 months**.

Good governance would dictate that the responsible entity should have a designated role or person who is responsible for ensuring reviews of the CIRMP are conducted regularly, and the frequency of these reviews should be informed by the changing environment.

9.2.2.2 Ensuring the CIRMP is up to date

Responsible entities are required to take all reasonable steps to ensure that the CIRMP is up to date (section 30AF of the SOCI Act). A component of meeting this requirement is reviewing and updating the CIRMP as circumstances change.

The CIRMP may not be considered up to date if it does not reflect the circumstances that the asset is currently operating in. Responsible entities should consider whether the CIRMP reflects the current:

- operating environment.
- threats and hazards relevant to the CI asset, including risk advice issued by Government.
- organisational structure and governance arrangements.
- regulatory requirements.
- lessons learned from relevant incidents.
- lessons learned from exercises or reviews.

9.2.3 What are reasonable steps?

Reasonable steps are explained in the glossary.

Responsible entities cannot elect not to implement a process for updating the CIRMP merely because it is inconvenient or expensive. The responsible entity should clearly demonstrate why they have not taken steps to update the CIRMP if they consider the steps to achieve this would not be reasonable.

9.2.4 What to consider when reviewing the CIRMP

When reviewing the CIRMP it is recommended that responsible entities consider whether the CIRMP is operating as intended and is effectively managing risks and hazards that threaten the CI asset.

To effectively manage risk, it is recommended that the CIRMP is appropriately supported by resources, capability, systems and oversight. This could include establishing appropriate governance practices and the CIRMP is being complied with internally, as is required in section 30AD of the SOCI Act.

Responsible entities should consider whether the CIRMP is still appropriate given the responsible entity's current operations, asset profile and risk environment. For example, the CI asset may have a change in level of risk exposure, and this should be reflected appropriately in the CIRMP.

9.2.5 Trigger based reviewing of the CIRMP

Trigger based reviews ensures that a responsible entity is considering new information as it becomes available and ensures that the CIRMP is fit for purpose to protect the CI asset from hazards. Trigger based reviews may be initiated by the matters set out in the list in section **9.2.7**, as well as in response to variations to the CIRMP. A responsible entity must take all reasonable steps to ensure their CIRMP is up to date. This could include reviewing their CIRMP if a hazard has a relevant impact on the CI asset that is not already described in the CIRMP.

9.2.5.1 Reviewing the whole CIRMP

There are many potential triggers that could cause a review to be required. Trigger based reviews are likely to only impact certain hazard vectors, however there may be circumstances that require a review of the entire program. Events that may indicate a review of the entire CIRMP is required include:

- A significant change to the asset or operations (for example major upgrades, decommissioning, changes in risk or systematic failure, etc.).
- Changes to the threat environment (for example emerging threats or attack vectors, increased geopolitical risks, etc.).
- Incidents that result in a relevant impact on the CI asset.
- A change to the asset's operating environment, ownership structure, or supply chain.
- A finding from an audit or assurance activity.
- As a result of a cyber security exercise or vulnerability assessment.
- Changes to regulatory or legislative environment.

Responsible entities should maintain an inventory of potential triggers for a full review of the CIRMP.

9.2.5.2 Reviewing a part of the CIRMP

Responsible entities may need to review parts of the CIRMP to ensure that it remains up to date. The changes to the items listed in **9.2.7** may trigger a partial review of the CIRMP. However this list is not exhaustive. There will be many other triggers for partial review of the CIRMP, and responsible entities should maintain an inventory of all of these potential triggers. They should also consider whether these triggers for partial review have cascading effects on other parts of the CIRMP, and those parts may also require review.



9.2.6 Establish and maintain a process or system to keep the CIRMP current to ensure compliance with 30AF of the SOCI Act

CIRMP baseline – section 30AF of the SOCI Act and section 7(1)(e) of the CIRMP Rules

CIRMP enhanced – section 30AF of the SOCI Act and section 7(1)(e) of the CIRMP Rules

TSRMP – section 30AF of the SOCI Act and section 9(e) of the TSRMP Rules

Responsible entities for CI assets subject to the baseline or enhanced CIRMP or the TSRMP must establish and maintain a process or system in their CIRMP to keep the CIRMP current to ensure compliance with section 30AF of the SOCI Act.

Section 30AF of the SOCI Act requires that if an entity is the responsible entity for one or more CI assets, and has adopted a CIRMP, then the entity must take all **reasonable steps** to ensure that the program is up to date. Non-compliance with this obligation attracts a civil penalty of 200 penalty units.

In this context reasonable steps may include actions such as:

- Establishing a formal review cycle
- Assigning clear ownership and accountability for maintaining the CIRMP
- Including the review of the CIRMP as a standing item at all risk management, security, or governance meetings
- Maintaining version control, change logs, and records of amendments made to the CIRMP
- Conducting periodic assurance reviews or internal audits to confirm the CIRMP remains accurate and reflects current operations
- Determining trigger based reviews – such as acquisitions, disposal or major modification of critical components of the CI asset
- Reassessing material risks at defined intervals to ensure the CIRMP address the risk appropriately
- Monitoring emerging risks and risk treatments

This is not an exhaustive list. Responsible entities should consider whether these actions are relevant to their CI asset, and what additional actions would comprise a reasonable step to ensure the program is up to date.

This obligation works together with the review the CIRMP on a regular basis (section 30AE of the SOCI Act) obligation to ensure meaningful uplift of the security and resilience of CI assets. This is only possible if the material risks and mitigations described in the CIRMP remain current.

This obligation to take all reasonable steps to ensure the CIRMP is up to date ensures that risk is being continually assessed and managed. The requirement to take all reasonable steps means the responsible entities must take steps that are reasonable in the circumstances that they are operating in. The extent to which the responsible entity's environment has varied will inform what would be considered a reasonable step. Responsible entities should consider evolving technology, business circumstances and the threat environment.

9.2.7 A responsible entity must have regard to certain matters in deciding to whether to adopt or vary the CIRMP

CIRMP baseline – section 30AKA of the SOCI Act

CIRMP enhanced – section 30AKA of the SOCI Act

TSRMP – section 30AKA of the SOCI Act

The SOCI Act requires responsible entities to have regard to certain matters when deciding whether to adopt or vary a CIRMP. These matters are prescribed throughout the CIRMP Rules and relate directly to the obligations under the CIRMP Rules.

When a responsible entity adopts, reviews, or varies their CIRMP, they must have regard to whether the CIRMP satisfies the items provided in the table below.

CIRMP Rules	Baseline requirements
All hazards	
s 7(2)(a)	Describe the outcome of the process or system to identify the operational context.
s 7(2)(b)	Describe interdependencies between the CI asset and other CI assets.
s 7(2)(c)	Identify positions responsible for developing and implementing the CIRMP, and reviewing or keeping it up to date.
s 7(2)(d)	Contains the contact details for the positions responsible for developing and implementing the CIRMP, and reviewing or keeping it up to date.
s 7(2)(e)	Contain a risk management methodology.
s 7(2)(f)	Describe the circumstances in which the entity will review the CIRMP.
Cyber and information security hazards	
s 8(6)	Describe the cyber and information security hazards that could have a relevant impact on the CI asset.
Personnel hazards	
s 9(6)(a)	List the entity's critical workers.
s 9(6)(b)	Describe the personnel risks which could have a relevant impact on the CI asset.
Supply chain hazards	
s 10(2)(a)	List the entity's major suppliers.
s 10(2)(b)	Describe the supply chain hazards which could have a relevant impact on the CI asset.
Physical security hazards and natural hazards	
s 11(2)(a)	Describe the CI asset's critical components.
s 11(2)(b)	Describe the physical security hazards which could have a relevant impact on a physical critical component.
s 11(2)(c)	Describe the security arrangements for the CI asset.
s 11(2)(d)	Describe the natural hazards which could have a relevant impact on the physical critical components.

Responsible entities subject to the enhanced CIRMP are required to have regard to all of the baseline items listed above, as well as the items listed below.

CIRMP Rules	Enhanced requirements
Cyber and information security hazards	
s 8A(5)	Contain appropriate measures that minimise or eliminate material risks to the CI asset including those specified at subsection 8A(2) of the CIRMP Rules.
Credential compromise hazards	
s 8B(6)(a)	Includes a process or system capable of outlining all of the systems and networks where phishing resistant multi-factor authentication is required under subsection 8A(3)(a).
s 8B(6)(b)	Describe credential compromise hazards that could have a relevant impact on the CI asset.
s 8B(6)(c)	Contain appropriate measures to minimise or eliminate material risks to the CI asset.
Lateral movement hazards	
s 8C(5)(a)	Describe the lateral movement hazards that could have a relevant impact on the CI asset.
s 8C(5)(b)	Include a process or system capable of identifying the matters specified at sections 8C(2)(a)-(c).
s 8C(5)(c)	Contains appropriate measures to minimise or eliminate material risks to the CI asset.
Personnel hazards	
s 9A(7)(a)	Contain appropriate measures that minimise or eliminate material risks to the CI asset, including those specified at section 9A(2) of the CIRMP Rules.
s 9A(7)(b)	Include a process or system capable of identifying the suitability of critical workers, and permitting them access to critical components only where found suitable.
Supply chain hazards	
s 10A(6)(a)	Include a process or system capable of identifying the matters specified at sections 10A(3)(a)-(c).
s 10A(6)(b)	The CIRMP includes a process or system capable of identifying the matters specified at sections 10A(5)(a)-(e).
Physical security hazards and natural hazards	
s 11A(4)	The CIRMP contains a system or process capable of identifying the matters specified at sections 11A(1)-(3).

To assist in ensuring these checks are conducted regularly, responsible entities are encouraged to keep track of when a review of each component took place.

The Department considers that a responsible entity should review its CIRMP in its entirety at least every 24 months.

9.3 Annual reporting requirements

Responsible entities are required to submit an annual report to the relevant Commonwealth regulator that has functions relating to the security of the responsible entity's assets (section 30AG of the SOCI Act). For critical financial market infrastructure assets, the relevant regulator is the Reserve Bank of Australia. For all other CI assets, the relevant regulator is the Department of Home Affairs.

Entities that fall under the exemptions in section 30AB(4), (5) and (6) of the SOCI Act (including assets that are HCF certified) are not subject to Part 2A and are therefore not required to adopt and maintain a CIRMP. However, if the entity is a responsible entity for one or more CI assets covered by section 30AB(4), (5) or (6), they are still subject to the annual reporting obligation in section 30AQ of the SOCI Act.

The annual report provides assurance to the relevant regulator that the responsible entity has complied with their CIRMP and has maintained a current program that appropriately identifies and manages material risks to the CI asset.

The annual report is not intended to duplicate the CIRMP. Instead, it is an assurance mechanism that provides visibility of how effectively the CIRMP is being implemented and maintained.

A single annual report is submitted per responsible entity, after the end of each financial year that a responsible entity has had a CIRMP, and may cover multiple CI assets.

9.3.1 What information must be included?

Responsible entities must provide the annual report in the approved form (section 30AG(2)(e) of the SOCI Act). The approved annual report form is updated annually to ensure the questions remain fit for purpose and aligned with the threat environment faced by CI assets. The update of the annual report form occurs within the first three months of the calendar year. The Department of Home Affairs will release guidance each year, to support the annual report form

> The annual report must be provided in the **approved form** and include sufficient information to demonstrate that the CIRMP is current and effective.

To comply with the requirements of the annual report in section 30AG(2) of the SOCI Act, the approved annual report form will always require:

- A statement as to whether or not the CIRMP was up to date at the end of the reporting period; and
- If there were any incidents where a hazard had a significant relevant impact on a responsible entity's CI asset(s) – a statement that:
    - identifies the hazard;
    - evaluates the effectiveness of the CIRMP in mitigating the significant relevant impact of the hazard on the asset(s); and
    - if the CIRMP was varied during the reporting period as a result of the hazard – outlines the variation.

If a declaration is made that the CIRMP is up to date, it is recommended that this is supported by evidence that the program has been reviewed and reflects the entity's current operating environment and risk profile.

It is also recommended that all responsible entities include in their annual report:

- A summary of any variations or updates made to the CIRMP during the reporting period, such as changes to risk assessments, controls, governance arrangements, or supporting documentation; and
- An assessment of whether the CIRMP has been effective in mitigating risks and managing impacts, taking into account lessons learned, incident outcomes, and any identified gaps or areas for improvement.

The annual report does not require submission of the CIRMP itself. However, the relevant regulator may request access to the CIRMP for compliance, assurance, or audit purposes.

9.3.2 Board approval

If the responsible entity has a board, council or governing body, the annual report must be approved by that responsible entity's board, council, or governing body prior to submission. If the responsible entity has more than one board, council, or governing body, the responsible entity must determine which body is most appropriate to provide the approval. The responsible entity is not required to obtain the approval from all bodies.

This requirement ensures that responsibility for the CIRMP is held at an appropriately senior level within the organisation. In the circumstance that an entity acts as the responsible entity for multiple CI assets, the responsible entity can elect to do an annual report for each CI asset, or a collective annual report for all CI assets governed by the responsible entity's board, council, or governing body.

It is recommended that the governing body approval confirms that:

- The CIRMP was in place and maintained during the reporting period.
- The information provided in the annual report is accurate and complete.
- The governing body has oversight of the entity's risk management practices.

It is best practice for the responsible entities to regularly report to their governing body, escalate any material risks, incidents, or gaps in a timely manner, and provide their governing body with sufficient information to support an informed approval process.

The annual reporting process provides an opportunity for boards, councils and governing bodies to review the effectiveness of the CIRMP, identify areas for improvement, and ensure that appropriate resources are allocated to manage risks.

9.3.3 Timeframes for submission

The reporting period for the annual report is the Australian financial year (1 July to 30 June).

Responsible entities must submit their annual report **within 90 days** after the end of the financial year. Non-compliance with this obligation may attract a civil penalty of 150 penalty units (section 30AG(2) of the SOCI Act)

It is recommended that responsible entities ensure that internal governance, review, and approval processes are scheduled in advance to enable timely submission. Failure to submit the report, or submitting it after the due date, constitutes non-compliance with the annual reporting obligation.

Where a responsible entity does not submit their annual report on time, the Department may engage directly with the entity to understand the reason for the delay, and request that the report is submitted as soon as practicable. The Department will also consider if enforcement action is appropriate.

The SOCI Act does not provide for extensions or exemptions from the annual reporting timeframe. Responsible entities are expected to ensure that appropriate internal processes are in place to enable timely submission.

Responsible entities should treat the annual reporting obligation as a key governance and assurance requirement and ensure that:

- Reporting timelines are incorporated into internal governance cycles.
- Sufficient time is allocated for review and board approval.
- Any risks to timely submission are identified and managed early.

Timely submission of the annual report supports effective engagement with Government and demonstrates that the responsible entity is maintaining an appropriate level of oversight of its critical infrastructure risk.



Table of contents: Attachment A

A 150
Absence or compromise 150
All hazards 150
Availability 150
B 150
Baseline CIRMP requirements 150
Business critical data 151
C 151
Computer 151
Confidentiality 151
Consequences 151
Cost 151
Credential 152
Credential compromise hazards 152
Critical component 152
Critical Infrastructure Risk Management Program (CIRMP) 153
Critical system 153
Critical worker 153
Cyber and information security hazards 154
E 154
Enhanced CIRMP requirement 154
Exploitation 154
F 154
Foreign ownership, control or influence 154
G 155
Grossly disproportionate 155
H 155
Have regard to 155
I 155
Impact 155
Integrity 155
Interference 155
International relations 155
Impairment 156
L 156
Lateral movement hazard 156
Likelihood 156
M 156
Major slowdown 156
Major supplier 156
Material risk 156
Maximum acceptable outage 157

N 157
National security 157
Natural hazard 157
O 158
Operational context 158
P 158
Personnel hazards 158
Phishing resistant multi-factor authentication 159
Physical security hazard 159
Prejudice 159
Proper function 159
R 159
Reasonable steps 159
Regular basis 160
Reliability 160
Relevant Commonwealth Regulator 160
Relevant official 160
Relevant impact 160
S 161
Security 161
Security assessment 161
Serious deficiency 161
Significant influence 161
So far as it is reasonably practicable 161
Stoppage 162
Supply chain 162
Supply chain hazards 162
T 162
Tier 1 supplier 162
Tier 2 supplier 162
Tier 3 supplier 162
Tier N supplier 162
U 163
Unauthorised access 163
Unmanageable period 163
User 163
V 163
Vendor 163

Attachment A: Glossary of terms

A

Absence or compromise

'Absence or compromise' is not defined in the SOCI Act or the CIRMP Rules. In the context of a 'critical worker' (in section 5 of the SOCI Act), 'absence or compromise' may refer to the person being unavailable to perform their duties (due to illness, resignation, being unreachable, etc) or the person's ability to perform their role is impaired, influenced or controlled by a malicious actor.

Relates to the definition of critical worker (section 5 of the SOCI Act).

All hazards

'All hazards' is not defined in the SOCI Act or the CIRMP Rules. The ordinary meaning of 'hazard' refers to a risk or exposure to danger or harm. The obligation on responsible entities to consider all hazards acknowledges that there is a broad spectrum of potential hazards faced by CI assets, and these hazards are interconnected in nature. 'All hazards' seeks to capture the complete risk environment that CI assets may face.

Availability

'Availability' is not defined in the SOCI Act or the CIRMP Rules. In the context of a 'relevant impact' it may include the ability of a critical infrastructure asset to remain accessible and operational when required. It may include essential services and systems being able to deliver their intended functions without undue interruption, even during incidents or disruptions.

B

Baseline CIRMP requirements

A 'baseline CIRMP' is defined in section 3 of the CIRMP Rules as any requirement specified in Part 2 of the CIRMP Rules for the purpose of section 30AH(2)(b) of the SOCI Act, other than an enhanced CIRMP requirement.

Throughout this guidance 'baseline CIRMP' is used to describe the obligation on CI assets that are not subject to the enhanced CIRMP requirements.

The entities subject to baseline CIRMP requirements are:

- Critical broadcasting assets
- Critical domain name systems
- Critical data storage or processing assets
- Critical electricity assets
- Critical energy market operator assets
- Critical gas assets
- Designated hospitals
- Critical food and grocery assets
- Critical freight infrastructure assets
- Critical freight services assets
- Critical liquid fuel assets
- Critical financial market infrastructure assets as specified in section 12D(1)(i) of the SOCI Act
- Critical water assets

Business critical data

'Business critical data' is defined in section 5 of the SOCI Act as:

- Personal information (within the meaning of the *Privacy Act 1988*) that relates to at least 20,000 individuals;
- Information relating to any research and development in relation to a critical infrastructure asset;
- Information relating to any systems needed to operate a critical infrastructure asset;
- Information needed to operate a critical infrastructure asset; or
- Information relating to risk management and business continuity (however described) in relation to a critical infrastructure asset.

C

Computer

'Computer' is defined in section 5 of the SOCI Act. A 'computer' means all or part of:

- One or more computers; or
- One or more computer systems; or
- One or more computer networks; or
- Any combination of the above.

This definition extends beyond the ordinary meaning of a computer. Examples include:

One or more computers.	A laptop, a bank of workstations, a single desktop.
One or more computer systems.	A cloud hosted customer relationship management system, an industrial control system managing manufacturing processes, systems consisting of application servers, databases, and storage
One or more computer networks.	A corporate local area network, the network connecting multiple branch offices of an organisation, the corporate Wi-Fi network
Any combination of the above.	An IT environment including laptops, desktops, HR and finance applications, and the corporate network connecting these systems A cloud environment consisting of multiple virtual machines, web application and database platforms, and a virtual network connecting resources.

It should be noted that the definition of a 'credential compromise hazard' uses the definition of computer provided here.

Confidentiality

'Confidentiality' is not defined in the SOCI Act or the CIRMP Rules. In the context of 'relevant impact' it may include to the protection of information from unauthorised access, disclosure, or misuse. Confidentiality applies to a range of information, which may include operational data, customer information, and security details that if exposed could increase vulnerability or lead to exploitation of the asset.

Consequences

'Consequence' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'consequence' is referred to as a secondary, often broader and longer-term outcome that arises from an impact. This could potentially include financial loss, reputational damage, or inability to provide critical services or functions. This term should be considered in relation to CIRMP when identifying, minimizing or eliminating material risks.

Cost

'Cost' is not defined in the SOCI Act or the CIRMP Rules. In the context of 'as far as reasonably practicable' it may include time, money, impact on productivity, or other resources.

Credential

'Credential' is not defined in the SOCI Act or in the CIRMP Rules. In the context of 'credential compromise' it may be interpreted as:

- information, or an associated object;
- that is used to verify the identity of a user, agents, system, or service; and
- that grants or enables access to a system, application, device or data.

Credentials establish a trusted link between an identity and an authenticator and may include attributes or permissions associated with that identity.

Credentials may take various forms, including passwords, cryptographic keys, tokens, certificates, or other authentication data, and may be associated with individuals, agents privileged users, systems, or automated processes.

Credential compromise hazards

'Credential compromise hazard' is defined in section 3 of the CIRMP Rules. A 'credential compromise hazard' is where credentials associated with:

- internet-connected computers or critical components; or
- remote access to those internet-connected computers or critical components;

are used to introduce vulnerabilities that could compromise the availability, integrity, reliability or confidentiality of the CI asset.

The definition provided above is exclusive, there are no other threats or hazards that are covered by credential compromise hazard.

Critical component

A 'critical component' is defined in section 5 of the SOCI Act. A 'critical component' is a part of a CI asset, where the absence of, damage to, or compromise of that part would prevent the proper function of the asset or could cause significant damage to the asset.

To manage risks associated with critical components responsible entities must have a thorough understanding of what components make up their CI asset. Critical components could include:

- Control rooms
- Gas pipelines
- Emergency shutdown valves
- Pump stations
- Water treatment reactors
- Mobile phone towers
- Fibre optic cables
- Life-support and medical equipment
- Patient monitoring systems
- Loading docks and transport hubs
- Temperature monitoring systems
- Critical systems
- Operational technology
- Enabling systems integral to the function of the asset

This is not a comprehensive list and critical components will vary based on asset type. For physical security hazards and natural hazards, responsible entities are required to identify physical critical components (see **8.2.1** of Chapter 8 – **Physical security and natural hazards**) and responsible entities subject to the enhanced CIRMP are required to identify critical systems for lateral movement hazards (see **5.2.1** of Chapter 5 – **Lateral movement hazards**).

Generally speaking, having a thorough understanding of all critical components of a CI asset will assist in appropriately managing risks to the CI asset, and ensuring compliance with SOCI obligations.

Critical Infrastructure Risk Management Program (CIRMP)

A 'critical infrastructure risk management program' (CIRMP) is defined in section 30AH of the SOCI Act. A CIRMP is a written program:

(a) that applies to a particular entity that is the responsible entity for one or more critical infrastructure assets; and

(b) the purpose of which is to do the following for each of those assets:

(i) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;

(ii) so far as it is reasonably practicable to do so—minimise or eliminate any material risk of such a hazard occurring;

(iii) so far as it is reasonably practicable to do so—mitigate the relevant impact of such a hazard on the asset; and

(c) that complies with such requirements (if any) as are specified in the Rules.

Critical system

A 'critical system' is defined in section 3 of the CIRMP Rules. 'Critical system' means any systems including operational technology or enabling systems that form critical components which are vital to the delivery of a CI asset's function, or the compromise or degradation of which could have a relevant impact on the asset.

Examples of critical systems in a cyber context may include:

- Programmable Logic Controllers or Remote Terminal Units used to control critical processes.
- Supervisory Control and Data Acquisition (SCADA) systems.
- Hardware supporting the operation of networks with critical systems, such as switches, firewalls and routers.
- Components used to provide backup power and functionality to critical systems and devices in emergency situations.

Critical worker

- A 'critical worker' is defined in section 5 of the SOCI Act. 'Critical worker' means an individual who is an employee, intern, contractor, or subcontractor of a responsible entity for a CI asset to which Part 2A applies, and who:
- the responsible entity assesses that the individual's absence or compromise would prevent the proper function of the CI asset or could cause significant damage to the CI asset; and
- the individual has access to, or control and management of, a critical component of the CI asset.

When considering the definition of a critical worker review the definitions of 'absence or compromise', 'critical component', and 'proper function'.

Whether someone is a critical worker depends on the **function** they perform. The person's seniority or length of service in the role is not determinative. For example, a short-term contractor may be a 'critical worker' despite not being an ongoing employee.

Information on identifying critical workers is in **6.2.1** of Chapter 6 - **Personnel hazards**.

Cyber and information security hazards

'Cyber and information security hazard' is defined in section 3 of the CIRMP Rules. 'Cyber and information security hazard' includes where a person, whether authorised or not:

- improperly accesses or misuses information or computer systems about or related to the CI asset; or
- uses a computer system to obtain unauthorised control of, or access to the CI asset that might impair its proper functioning.

A cyber and information security hazard can also include any relevant hazard that may have an impact on the cyber and information security of a critical infrastructure asset.

For example:

- Prepositioning in the IT or OT of a CI asset, regardless of whether there has been any negative impact to the function of the CI asset.
- Use of Artificial Intelligence (AI) against the asset or by the asset which may impact the function of the CI asset.
- The impacts of redundant or unsupported technology on the CI asset.

E

Enhanced CIRMP requirement

'Enhanced CIRMP requirement' is defined in section 3 of the CIRMP Rules. 'Enhanced CIRMP requirement' means a requirement specified in section 4A(5) of the CIRMP Rules.

Throughout this guidance 'enhanced CIRMP' is used to describe the obligations on CI assets that are subject to the enhanced CIRMP obligations These are entities specified in section 4A(1) of the CIRMP Rules.

Exploitation

'Exploitation' is not defined in the SOCI Act or the CIRMP Rules. In the context of supply chain material risks, 'exploitation' may refer to deliberate use of supply chain relationships, vulnerabilities or dependencies to gain advantage or enable further compromise of the asset. Exploitation could occur from someone from within the supply chain, or an external party.

Exploitation may include:

- A threat actor deliberately targeting a lower security supplier to gain a foothold and then move laterally through their systems to disrupt the CI asset.
- Using a supply chain dependency to apply pressure or coerce a responsible entity.
- Leveraging supplier relationships to conduct espionage and pre-position for future malicious activity.

F

Foreign ownership, control or influence

FOCI is defined in section 3 of the CIRMP Rules as meaning foreign ownership, control or influence (FOCI).

FOCI risk refers to the ability for vendors to be directed by a foreign government, either through direct ownership channels, the domestic laws of a foreign jurisdiction or outside influence (such as political party membership) to conduct malicious activities on behalf of that government.

FOCI risk can be present when, for example, a vendor is exposed to a foreign state through either ownership, control, or influence.

Foreign ownership: May refer to the degree to which foreign countries possess ownership stakes in a company, its subsidiaries, and its affiliates. This could involve a portion of the company's shares being held under foreign investment by a foreign person, foreign resident, or that a foreign company has significant equity interest. Foreign investments can also come through venture capital.

Foreign control: May refer to the authority and influence exerted by foreign entities and governments over a company's decision-making processes. This can involve legislation allowing the use and access of data and communications generated and stored by industry in a foreign country, the appointment of key personnel or board members, or other measures that grant foreign interests a say in how the company operates.

Foreign (malign) influence: Can be applied on vendors or other entities through various coercive means, including economic leverage, strategic partnerships, or even subtle political manoeuvring. When foreign actors or governments seek to exert influence in a way that is actively hidden or not transparent, this can have serious implications for organisations and Australia.

Vendors or other entities subject to FOCI can be directed to act against their own business interests. They could be compelled by a foreign government to conduct malicious acts such as undermining the security of their products and services or providing privileged access to systems and client data to unauthorised agents. Such influence, if not properly managed, can lead to unauthorised access to sensitive information or negatively impact performance and contracts. Managing FOCI risk extends beyond national security; it allows responsible entities to protect their organisation's reputation, their organisation's systems and intellectual property, their business interests, and the privacy of their staff and customers.

G

Grossly disproportionate

'Grossly disproportionate' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'grossly disproportionate' may refer to circumstances where the cost, effort, time or other sacrifice required to address a risk is clearly excessive when compared to the likelihood and consequence of that risk.

H

Have regard to

'Have regard to' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'have regard to' may refer to an obligation to genuinely consider, take into account, and give appropriate weight to a matter that is relevant to a decision, assessment, or course of action.

Whether sufficient regard has been given will depend on the circumstances and the nature of the matter being considered. Having regard to a matter does not require a responsible entity to adopt a particular outcome or give the matter determinative weight. However, the responsible entity should be able to demonstrate that the matter was actively considered and informed its decision-making process.

I

Impact

'Impact' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'impact' may refer to a noticeable or marked effect on a critical infrastructure asset, its functions, services, systems, operations or security.

For the definition of **relevant impact** see below.

Integrity

'Integrity' is not defined in the SOCI Act or the CIRMP Rules. In the context of 'relevant impact', 'integrity' may include assurance that critical infrastructure assets and the essential functions operate as intended, without unauthorised or unintended alteration. This might include maintaining the accuracy of systems, processes, data, and physical components so they deliver safe and reliable outcomes even under stress or threat.

Interference

'Interference' is not defined in the SOCI Act or the CIRMP Rules. In the context of supply chain material risks, 'interference' may include action that alters, disrupts, degrades or impacts the functioning of a CI asset or its critical component through the supply chain. Interfering with the CI asset's supply chain may look like:

- Tampering with hardware or software during manufacturing, transit, or delivery phases which introduces unreliable components to the CI asset.
- Disruption to the delivery of goods preventing timely access to critical parts or maintenance.
- Introduction of malicious updates of patches which are then deployed to operating systems.

International relations

'International relations' is defined in section 5 of the SOCI Act. 'International relations' means political, military and economic relations with foreign governments and international organisations.

Impairment

'Impairment' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'impairment' may refer to something being made worse, diminished or adversely affected.

L

Lateral movement hazard

'Lateral movement hazard' is defined in section 3 of the CIRMP Rules. 'Lateral movement hazard' means a hazard where a computer is used by a user (whether authorised or otherwise) to move between computer systems to critical systems, or between two critical systems, which could compromise the availability, integrity, reliability or confidentiality of the CI asset.

The definition provided above is exclusive, there are no other threats or hazards that are covered by lateral movement hazard.

Likelihood

'Likelihood' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'likelihood' may refer to the chance of something happening, as supported by evidence or research.

M

Major slowdown

‘Major slowdown' is not defined in the SOCI Act or the CIRMP Rules. In the context of section 6(a) of the CIRMP Rules, 'major slowdown' may refer to a significant degradation of a CI asset's ability to deliver its functions.

Major supplier

'Major supplier' is defined in section 3 of the CIRMP Rules. 'Major supplier' means any vendor that, by nature of the product or service they offer, has a significant influence over the security of a responsible entity's CI asset.

When determining whether an entity is a major supplier, three factors should be considered:

- Whether the entity is a vendor;
- The product or service the vendor offers; and
- Whether, by nature of that product or service, the vendor holds a significant influence over the security of a responsible entity’s CI asset.

When considering the definition of a major supplier review the definitions of ‘vendor’ and ‘significant influence’.

Material risk

'**material risk**' is not specifically defined in the SOCI Act or the CIRMP Rules. ‘Material’ and ‘risk’ are given their ordinary meaning according to the Macquarie Dictionary.

A material risk might be a risk that extends beyond routine operational issues and could disrupt essential services, compromise national security, or cause significant consequences for a CI asset. Material risks may stem from a routine issue that evolves or has the potential to disrupt or compromise the critical infrastructure asset and have cascading effects across other sectors.

As set out in s 30AH(7) of the SOCI Act, in determining whether a risk is a material risk, regard must be had to the likelihood of the hazard occurring and the relevant impact of the hazard on the asset if the hazard were to occur.

Sections 6 and 6A of the CIRMP Rules and s 8 of the TSRMP specify particular risks that must be taken to be material risks for the purposes of a responsible entity’s CIRMP. Those are set out in **Attachment B**.

More information on material risks can be found in Chapter 1 – **Introduction to the critical infrastructure risk management program (CIRMP)**.

Maximum acceptable outage

'Maximum acceptable outage' is defined in section 3 of the CIRMP Rules. 'Maximum acceptable outage' means the maximum period of time for which a critical component, service or other thing for the CI asset can be unavailable without unreasonably disrupting the ongoing availability, integrity, reliability or confidentiality of the CI asset.

An outage may be created through the unavailability of products or services from providers or vendors. Having a thorough understanding of the critical components, major suppliers, and proper function of the CI asset will allow the responsible entity to determine what the maximum acceptable outage for the CI asset is, and how the major suppliers may impact this period. The maximum acceptable outage may also be informed by mitigations. For example, if an entity has a large stockpile of an important product, it is likely that the maximum acceptable outage would be longer, as the entity will be able to rely on the stockpile.

In considering what the maximum acceptable outage is, considerations may include:

- Whether there are any regulatory or contractual obligations (such as Service-Level Agreements) that mandate minimum uptimes.
- Whether redundancy mechanisms (such as parallel systems, spare parts, backups, or alternative vendors) are available, tested and ready to use.
- Impacts to the safety of operations as a result of downtime.
- How long the relevant system, service or thing could continue without an impact to downstream customers and the community at large.

N

National security

'National security' is defined in section 5 of the SOCI Act. 'National security' means Australia's defence, security or international relations.

When considering the definition of a national security review the definitions of ‘security’ and ‘international relations’.

Natural hazard

'Natural hazard' is defined in section 3 of the CIRMP Rules. 'Natural hazard' includess fire, flood, cyclone, storm, heatwave, earthquake, tsunami, space weather or a biological health hazard (such as a pandemic).

A natural hazard can also include any relevant, naturally occurring hazard that may have an impact on the physical security of a critical infrastructure asset.

O

Operational context

'Operational context' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'operational context' may refer to the environment in which a CI asset operates, including its systems, people, processes, dependencies and external factors that influence its functioning.

The operational context will be informed by:

- Internal environment – including things like the IT/OT systems, processes and procedures, workforce capability, and governance and management structures.
- External environment – including things like the threat landscape, regulatory and legal requirements, supply chain and third party dependencies, and interdependencies with other CI assets.

Internal environment

Understanding the internal operational context will allow the responsible entity to understand the complexities of their operating environment and identify the core requirements for the CI asset. Some assets are likely to have a significant amount of OT, and this would inform their approach to cyber security. Other assets may be highly reliant on critical workers, and this would emphasise the importance of a strong personnel management framework. Understanding the operational context ensures the responsible entity has an understanding of the fundamental requirements for their CI asset, and what risks may be present as a result.

External environment

When considering the external environment, it is recommended that the responsible entity consider the political, environmental, geographical, supply chain and other externals factors that impact the CI asset, or the responsible entity.

The CI asset may be located in a geographical location subject to significant natural disasters. This would impact the way that asset operates, and how it implements risk mitigations.

The ownership structure of a CI asset, including the degree of foreign ownership, control, or influence over the responsible entity will also inform the operational context for a CI asset. For example, a CI asset may rely on technology from overseas entities. This may introduce additional considerations such as foreign regulatory obligations, geopolitical developments, or supply chain disruptions. Understanding these relationships will assist the responsible entity in assessing risk and implementing governance and controls.

Similarly, the supply chain of the CI asset, or interdependencies have an impact on the operational context of the asset. For example, a critical water asset may only have one supplier for a vital product. This information would inform the operational context of the CI asset and it is recommended that the responsible entity consider this.

A CI asset's operational context will inform the risks and mitigations for the responsible entity.

P

Personnel hazards

'Personnel hazard' is defined in section 3 of the CIRMP Rules. 'Personnel hazard' includes where a critical worker acts, through malice or negligence, to compromise the proper function of the asset or cause significant damage to the asset.

A personnel hazard can also include any relevant personnel hazard that may have an impact on the security of a critical infrastructure asset.

Phishing resistant multi-factor authentication

'Phishing resistant multi-factor authentication' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'phishing resistant multi-factor authentication' refers to authentication methods designed to prevent the misuse of credentials obtained through phishing and similar attacks.

Multi-factor authentication (MFA) is a method of authentication that uses two or more authenticating factors to authenticate a single claimant to a single authentication verifier.

Phishing is a form of social engineering in which malicious actors use email or websites to solicit information. An example of this may be a person receiving an email requesting they log into their bank account via a link. The person uses the link provided in the email, which leads them to an illegitimate website, where they then enter their username, password, and authenticate the action via an SMS. The use of non-phishing resistant MFA, such as SMS verification, does not protect a person's credential when they willingly authenticate through non-phishing resistant MFA methods.

Phishing resistant MFA is a mechanism that cannot be defeated by credential replay or relay attacks.

Key characteristics of phishing resistant MFA include strong cryptographic methods, biometric verifications, and mutual authentication between user and the service.

For example, a critical worker has personalised credentials for a critical system. This critical system uses traditional MFA and sends an SMS to the worker's mobile device to gain verification. The worker's credentials have been compromised through a phishing attack. A malicious actor then uses the login credentials and sends countless authentication requests through to the critical worker. The critical worker is confused and eventually verifies the log in attempt. The malicious actor now has access to the critical system.

Some examples of phishing resistant MFA include:

- Fast Identity Online version 2 (FIDO2) passkeys and hardware keys
- Public Key Infrastructure (PKI)-based MFA
- Personal identity verification and common access cards
- Certificate-based authentication and smart cards
- Platform authenticators using FIDO2

Physical security hazard

'Physical security hazard' is defined in section 3 of the CIRMP Rules. 'Physical security hazard' includes unauthorised access to, interference with, or control of a CI asset, to compromise the proper function of the asset or cause significant damage to the asset.

A physical security hazard can also include any relevant hazard that may have an impact on the physical security of a critical infrastructure asset.

Prejudice

'Prejudice' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'prejudice' may refer to adversely affecting, disadvantaging or detrimentally impacting a person, asset, interest or outcome.

Proper function

'Proper function' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'proper function' may refer to the ability of a CI asset to deliver its essential service in a manner that maintains the availability, reliability, integrity and confidentiality of the asset.

R

Reasonable steps

'Reasonable steps' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'reasonable steps' will depend on the individual circumstances of the CI asset, the security environment, and the extent of the updates required.

What a reasonable step will be for a responsible entity will vary depending on the size and maturity of the CI asset, the practicality of taking the steps, and the level of risk being addressed by the steps.

Regular basis

‘Regular basis’ is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'regular basis' may refer to activities occurring consistently and repeatedly over time, rather than as a one-off or ad hoc occurrence. Generally, it does not require a daily basis but implies a pattern or frequency that is predictable and ongoing.

‘Regular basis’ is used in relation to the review of the CIRMP. The use of this term, rather than a defined timeframe, acknowledges the differing threat environments faced by CI assets and provides the responsible entity with a degree of discretion to determine the frequency with which reviews should occur. Consideration should be paid to the context in which the CI asset operates under.

Reliability

'Reliability' is not defined in the SOCI Act or the CIRMP Rules. In the context of a relevant impact, 'reliability' may refer to the consistent and dependable performance of a critical infrastructure asset. This could include the capacity to meet service obligations under usual and adverse conditions, minimising failures that could lead to an impact on national security, economy or public safety.

Relevant Commonwealth Regulator

Relevant Commonwealth regulator is defined in section 5 of the SOCI Act and means either a Department that is specified in the Rules or a body that is established by a law of the Commonwealth and is specified in the Rules.

Section 5 of the CIRMP Rules specifies the Reserve Bank of Australia as the relevant Commonwealth regulator for certain critical financial market infrastructure assets (see s 12D(1)(i) of the SOCI Act and s 10(5) of the *Security of Critical Infrastructure (Definitions) Rules 2021*).

No other relevant Commonwealth regulator has been specified.

Relevant official

'Relevant official' is defined in section 30AI(2) of the SOCI Act. 'Relevant official' means the Secretary of the Department of Home Affairs, or the chief executive officer or senior executive service employee (or equivalent, including acting, or higher), at a relevant Commonwealth regulator that has functions relating to the security of the asset.

Relevant impact

‘Relevant impact’ is defined in section 8G of the SOCI Act as a direct or indirect impact of a hazard or incident (including a cyber security incident) on the availability, integrity, or reliability of a CI asset or a direct or indirect impact of an incident (including a cyber security incident) on the availability, integrity, or reliability of a system of national significance (SoNS).

It also includes a direct or indirect impact of a hazard (on a CI asset) or an incident (on a CI asset or SoNS) on the confidentiality of:

- Information about the asset or system; or
- If information is stored in the asset or system – the information; or
- If the asset or system is computer data – the computer data.

When considering the definition of a relevant impact review the definitions of ‘*availability*’, ‘*integrity’*, ‘*reliability*’ and ‘*confidentiality’*.

S

Security

‘Security’ is defined in section 5 of the SOCI Act as (other than in references to national security), having the same meaning as in the ASIO Act and, in some circumstances, its ordinary meaning.

The ASIO Act defines ‘security’ as:

(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:

(i) espionage;

(ii) sabotage;

(iii) politically motivated violence;

(iv) promotion of communal violence;

(v) attacks on Australia’s defence system; or

(vi) acts of foreign interference;

whether directed from, or committed within, Australia or not; and

(aa) the protection of Australia’s territorial and border integrity from serious threats; and

(b) the carrying out of Australia’s responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

The ordinary meaning of ‘security’ includes:

- Freedom from danger, risk, etc.
- Freedom from care apprehension, or doubt.
- Something that secures or makes safe, such as a protection or defence.

Security assessment

'Security assessment' has the same meaning as in section 35(1) of the ASIO Act. ‘Security assessment’ means a statement in writing furnished by ASIO to a Commonwealth agency, State or authority of a State expressing any recommendations, opinion or advice on, or otherwise referring to, the question whether it would be consistent with the requirements of security for prescribed administrative action to be taken in respect of a person or the question whether the requirements of security make it necessary or desirable for prescribed administrative action to be taken in respect of a person, and includes any qualification or comment expressed in connection with any such recommendation, opinion or advice, being a qualification or comment that relates or that could relate to that question.

‘Prescribed administrative action’ in this context relevantly includes action that relates to or affects:

- access by a person to any information or a place access to which is controlled or limited on security grounds; or
- a person’s ability to perform an activity in relation to, or involving, a thing (other than information or a place), if that ability is controlled or limited on security grounds.

Serious deficiency

'Serious deficiency' is defined in section 30AI(3) of the SOCI Act. 'Serious deficiency' is a deficiency that poses a material risk to Australia's national security, defence, or the social or economic stability of Australia and its people.

Significant influence

'Significant influence' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'significant influence' may refer to the capacity of a person, supplier or vendor to materially affect the security, operation or outcomes of a critical infrastructure asset.

So far as it is reasonably practicable

'So far as it is reasonably practicable' is not defined in the SOCI Act or the CIRMP Rules. In the context of the CIRMP obligations, the term should be considered to be an objective legal standard requiring a responsible entity to do what a reasonable person would do to eliminate or minimise risk, unless the cost is grossly disproportionate to that risk.

The process for assessing “so far as it is reasonably practicable” is provided in Chapter 1 – **Introduction to the critical infrastructure risk management program (CIRMP)** of this guidance.

Stoppage

'Stoppage' is not defined in the SOCI Act or the CIRMP Rules. In the context of section 6(a) of the CIRMP Rules, 'stoppage' may refer to the loss or cessation of a CI asset's ability to perform its functions.

Supply chain

'Supply chain' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'supply chain' may refer to a network of entities, processes, financial flows and technologies involved in the production, delivery, and maintenance of goods and services that support the operation of a critical infrastructure asset. Supply chains are a continuum – a CI asset will likely have a supply chain it depends on and may also form part of *another* CI asset's supply chain.

It is important to note that a supply chain can be physical (such as freight infrastructure, supply of physical goods and services) and it can also involve the provision of non-physical services (such as managed services, data storage or processing, administrative services, software, remote monitoring, diagnostics and technical support.). Responsible entities should consider where their data is stored and how this may constitute part of their supply chain. This would include data storage providers, as well as other providers that store data such as legal providers or other professional services that hold significant amounts of business critical data.

Equipment moving between environments (such as out of the control of the organisation or offshore) may be part of the supply chain of a CI asset.

Supply chain hazards

'Supply chain hazard' is defined in section 3 of the CIRMP Rules. 'Supply chain hazard' includes malicious people both internal and external exploiting, misusing, accessing or disrupting the supply chain and over-reliance on particular suppliers.

A supply chain hazard may also include other relevant hazards that may have an impact on the supply chain of a critical infrastructure asset. For example, a flood may have a significant impact on an entity's supply chain, and this may be a supply chain hazard as well as a natural hazard. Responsible entities should consider supply chain impacts that may stem from all hazards.

T

Tier 1 supplier

'Tier 1 supplier' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'Tier 1 supplier' refers to a supplier that provides goods or services directly to the responsible entity.

Tier 2 supplier

'Tier 2 supplier' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'Tier 2 supplier' refers to a supplier that provides goods or services to a Tier 1 supplier.

Tier 3 supplier

'Tier 3 supplier' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'Tier 3 supplier' refers to a supplier that provides goods or services to a Tier 2 supplier.

Tier N supplier

'Tier N supplier' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'Tier N supplier' refers to all supply chain layers beyond Tier 3 suppliers.

U

Unauthorised access

‘Unauthorised access’ in relation to section 10(1)(i) of the CIRMP Rules (supply chain specified material risks) is not defined in the SOCI Act or the CIRMP Rules. In the context of supply chain material risks, ‘unauthorised access’ refers to any access to systems, data, facilities, or components of a CI asset that is not permitted or approved. In this context, unauthorised access to a CI asset’s supply chain may look like:

- An external actor gaining access to a vendor’s IT system, which allows insertion of malicious code that is later deployed into the CI asset
- Unauthorised access to a logistics provider’s tracking systems which enable the manipulation of delivery schedules of important materials.
- Unauthorised access to a manufacturer’s production systems which enables tampering with components prior to delivery.

Unmanageable period

‘Unmanageable period' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'unmanageable period' may refer to the period of time where a stoppage or major slowdown prevents the function of the CI asset and cannot be managed by reasonable contingencies or response and recovery measures.

An unmanageable period will likely be reached when the stoppage or major slowdown has had, or is having, a relevant impact on the CI asset.

The following are examples of when a stoppage or major slowdown may last for a period which is unmanageable:

- Maximum acceptable outage is exceeded (for example outage lasts longer than the asset can safely or reliably operate without service) – for more information on **maximum acceptable outage** see the Glossary.
- Contingencies fail or are exhausted (backup systems, manual workarounds, or redundancies can no longer sustain service)
- Recovery cannot be achieved within planned time objectives (for example, exceeds the maximum acceptable outage).
- Impacts escalate to having a relevant impact on the CI asset.

User

'User' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'user' means any individual, organisation, system, service, account, process or device that can access, interact with, or initiate activity on a computer or computer system, whether authorised or unauthorised.

V

Vendor

'Vendor' is not defined in the SOCI Act or the CIRMP Rules. In the context of this guidance, 'vendor' may refer to a provider of goods or services to a responsible entity of a CI asset.

Vendors should be considered across multiple levels of the supply chain. For example, a vendor may provide a piece of equipment. This piece of equipment comprises of multiple components from other vendors. All of these vendors supply to the CI asset. A vendor can be the manufacturer, integrator, installer, or reseller of a good or service.

Attachment B: Glossary of material risks

The below list details all specified material risks in the CIRMP Rules. Information on these risks is provided throughout the guidance. This list should be used as supporting material, and responsible entities should refer to the CIRMP Rules where possible.

Hazard Category	Material Risk	Reference		
		Baseline	Enhanced	TSRMP
All Hazards	A stoppage or major slowdown of the CI asset's function for an unmanageable period.	s 6(a)	s 6(a)	s 8(a)
All Hazards	A substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the CI asset. *Example:* The position, navigation and timing systems affecting provision of service or functioning of the asset.	s 6(b)	s 6(b)	s 8(c)
All Hazards	An interference with the CI asset's operational technology or information communication technology essential to the functioning of the asset. *Example (baseline and enhanced):* A Supervisory Control and Data Acquisition (SCADA) system. *Example (TSRMP):* A billing and charging system.	s 6(c)	s 6(c)	s 8(d)
All Hazards	The storage, transmission or processing of sensitive operational information outside Australia, which includes: • layout diagrams • schematics • geospatial information • configuration information • operational constraints or tolerances information • data that a reasonable person would consider to be confidential or sensitive about the asset.	s 6(d)	s 6(d)	s 8(e)
All Hazards	Remote access to operational control or operational monitoring systems of the CI asset.	s 6(e)	s 6(e)	s 8(f)
All Hazards	Impact to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data.	s 6(f)	s 6(f)	s 8(i)
All Hazards	Any impairment of the functions of the CI asset that could prejudice the social stability, economic stability, national security or defence of Australia.		s 6A(2)(a)	
All Hazards	Compromise or impairment of the functions of the CI asset as a result of, or in connection with FOCI.		s 6A(2)(b)	
All Hazards	Offshore or remote access to critical components.		s 6A(2)(c)	
All Hazards	Offshore or remote access to business critical data.		s 6A(2)(d)	
All Hazards	An impairment of the relevant CI asset's functions that prejudices the social or economic stability, or national security of Australia.			s 8(b)

Hazard Category	Material Risk	Reference		
		Baseline	Enhanced	TSRMP
All Hazards	Compromise, theft or manipulation of communications.			s 8(g)
All Hazards	Unauthorised use which compromises the security and function of a relevant CI asset, including by a: • Major supplier • Critical worker or • Managed service provider. *Example*: Software installed by a major supplier on a modem without the knowledge of the responsible entity.			s 8(h)
Cyber and Information	Failure to patch or update operating or security systems in a timely manner.		s 8A(2)(a)	
Cyber and Information	Failure to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued.		s 8A(2)(b)	
Cyber and Information	Deployment or hosting of advanced, novel or emerging technology in a manner that could prejudice the availability, integrity, reliability or confidentiality of the CI asset.		s 8A(2)(c)	
Cyber and Information	Use of advanced, novel or emerging technology against the asset, in a manner that could prejudice the availability, integrity, reliability or confidentiality of the CI asset.		s 8A(2)(d)	
Personnel	Arising from malicious or negligent employees or contractors.	s 9(1)(c)(i)	s 9(1)(c)(i)	s 12(c)(a)
Personnel	Arising from the off-boarding process for outgoing employees and contractors.	s 9(1)(c)(ii)	s 9(1)(c)(ii)	s 12(c)(b)
Personnel	Unauthorised or unsupervised access to critical components.		s 9A(2)(a)	
Personnel	The compromise or misuse of credentials and privileged access used by individuals to access the CI asset.		s 9A(2)(b)	
Personnel	Access to the CI asset by persons other than critical workers for the CI asset.		s 9A(2)(c)	
Personnel	Incoming and outgoing critical workers.		s 9A(2)(d)	
Supply Chain	Unauthorised access, interference or exploitation of the asset's supply chain.	s 10(1)(a)(i)	s 10(1)(a)(i)	s 14(1)(a)(i)
Supply Chain	Misuse of privileged access to the asset by any provider in the supply chain.	s 10(1)(a)(ii)	s 10(1)(a)(ii)	s 14(1)(a)(ii)
Supply Chain	Disruption of the asset due to an issue in the supply chain.	s 10(1)(a)(iii)	s 10(1)(a)(iii)	s 14(1)(a)(iii)
Supply Chain	Arising from threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains.	s 10(1)(a)(iv)	s 10(1)(a)(iv)	s 14(1)(a)(iv)

Hazard Category	Material Risk	Reference		
		Baseline	Enhanced	TSRMP
Supply Chain	Arising from major suppliers.	s 10(1)(a)(v)	s 10(1)(a)(v)	s 14(1)(a)(v)
Supply Chain	Any failure or lowered capacity of other assets and entities in the entity's supply chain.	s 10(1)(a)(vi)	s 10(1)(a)(vi)	s 14(1)(a)(vi)
Physical and Natural	A physical security hazard on a physical critical component.	s 11(1)(b)(i)	s 11(1)(b)(i)	s 15(1)(b)(i)
Physical and Natural	A natural hazard on the CI asset.	s 11(1)(b)(ii)	s 11(1)(b)(ii)	s 15(1)(b)(ii)

Attachment C – Checklists for CIRMP obligations

About this checklist

These checklists are intended as a practical self-assessment tool to assist responsible entities in considering their obligations under the ***Security of Critical Infrastructure Act 2018*** (SOCI Act) and the ***Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023*** (CIRMP Rules). It consolidates the CIRMP requirements into a single document to support responsible entities in assessing their CIRMP arrangements against the obligations.

The checklist is designed for **internal use by responsible entities** to help identify, monitor and review compliance with CIRMP obligations. It may support governance, risk management and continuous improvement activities, but it is not mandatory to use.

The checklist should not be relied on as evidence of compliance. Compliance with CIRMP obligations requires responsible entities to establish, implement, maintain, and review their CIRMP. Additional supporting evidence may be necessary to demonstrate compliance.

Responsible entities should use this checklist as a guide only and refer to the SOCI Act and CIRMP Rules.

Understanding the checklist

Some rows in this checklist are intentionally staggered beneath other rows. This reflects the structure of the CIRMP Rules and is designed to help users understand how individual obligations relate to broader requirements.

The staggered layout is intended to:

- show the relationship between higher-level obligations and their supporting requirements;
- preserve the structure and context of the CIRMP Rules;
- assist responsible entities to identify all relevant components of an obligation; and
- reduce the risk of overlooking specific requirements that sit beneath a broader legislative provision.

Where an obligation contains multiple subordinate obligations, responsible entities should consider each staggered row individually when assessing their compliance. The parent row provides context, while the staggered rows identify the specific matters that should be addressed.

If the responsible entity is subject to the baseline CIRMP they should refer to pages 2 - 7

If the responsible entity is subject to the enhanced CIRMP they should refer to pages 8 - 22

Baseline CIRMP obligation	Content in this colour relates to the obligation immediately above it
Enhanced CIRMP obligation	Content in this colour relates to the obligation immediately above it

The grace periods provided in the below checklists only apply to entities that were a CI asset subject to Part 2A obligations prior to the commencement of the amendment to the CIRMP.

Checklists for baseline CIRMP

All hazards		Chapter 2	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
s 6 and 7(1)	**A responsible entity must establish and maintain a process or system in the entity's CIRMP:**		
s 7(1)(a)	To identify the operational context of the CI asset.	**Nil**	
s 7(1)(b)	To identify the material risks to the CI asset.	**Nil**	
s 7(1)(c)	As far as it is reasonably practicable to do so: • to minimise or eliminate the material risks, which may include those mentioned in sections 6 and 6A; and • to mitigate the relevant impact of each hazard on the CI asset.	**Nil**	
s 6(a)	To minimise or eliminate the material risk of a stoppage or major slowdown of the CI asset's function for an unmanageable period.	**Nil**	
s 6(b)	To minimise or eliminate the material risk of a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the CI asset.	**Nil**	
s 6(c)	To minimise or eliminate the material risk of an interference with the CI asset's operational technology or information communication technology essential to the functioning of the asset. *Example A Supervisory Control and Data Acquisition SCADA system.*	**Nil**	
s 6(d)	To minimise or eliminate the material risk of the storage, transmission or processing of sensitive operational information outside Australia, which includes: • layout diagrams; • schematics; • geospatial information; • configuration information; • operational constraints or tolerances information; • data that a reasonable person would consider to be confidential or sensitive about the asset;	**Nil**	
s 6(e)	To minimise or eliminate the material risk of a remote access to operational control or operational monitoring systems of the CI asse	**Nil**	
s 6(f)	To minimise or eliminate the material risk of a impact to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data.	**Nil**	
s 7(1)(d)	To review the CIRMP to ensure compliance with section 30AE [Review of critical infrastructure risk management program] of the Act.	**Nil**	
s 7(1)(e)	To keep the CIRMP current to ensure it complies with section 30AF [Update of critical infrastructure risk management program] of the Act.	**Nil**	

s 7(2)	In deciding to adopt, review or vary a CIRMP, a responsible entity must have regard to whether the CIRMP:		
s 7(2)(a)	Describes the outcome of the process or system to identify the operational context.	**Nil**	
s 7(2)(b)	Describes interdependencies between the entity's CI asset and other CI assets.	**Nil**	
s 7(2)(c)	Identifies each position within the entity: • that is responsible for developing and implementing the CIRMP and • that is responsible for reviewing or keeping the CIRMP up to date.	**Nil**	
s 7(2)(d)	Contains the contact details for the positions responsible for the CIRMPs development, implementation, review or maintenance.	**Nil**	
s 7(2)(e)	Contains a risk management methodology.	**Nil**	
s 7(2)(f)	Describes the circumstances in which the entity will review the CIRMP.	**Nil**	

Cyber and Information Security Hazard		Chapter 3	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
s 8(2)	**A responsible entity must establish and maintain a process or system in the CIRMP to—as far as it is reasonably practicable to do so:**		
s 8(2)(a)	Minimise or eliminate any material risk of a cyber and information security hazard occurring.	**Nil**	
s 8(2)(b)	Mitigate the relevant impact of a cyber and information security hazard on the CI asset.	**Nil**	
s 8(4) and (5)	**A responsible entity must establish and maintain a process or system in the CIRMP to:**		
s 8(4)(a) **s 8(5)**	Comply with a framework [or alternative equivalent framework (section 8(5))] contained in a document mentioned in the table in section 8(4) as in force from time to time.	**Nil**	
s 8(4)(b)	Meet any conditions mentioned in the table in section 8(4) for the document.	**Nil**	
s 8(6) and s8A(5)	**In deciding to adopt, review or vary a CIRMP, a responsible entity must have regard to whether the CIRMP.**		
s 8(6)	Describes the cyber and information security hazards that could have a relevant impact on the asset.	**Nil**	

Personnel Hazards		Chapter 6	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
s 9(1)	**A responsible entity must establish and maintain a process or system in the entity's CIRMP:**		
s 9(1)(a)	To identify the entity's critical workers;	**Nil**	
s 9(1)(b)	To permit a critical worker access to critical components of the CI asset only where the critical worker has been assessed to be suitable [suitability assessments may include an AusCheck background check, in which case responsible entities must include an assessment in accordance with section 9(3). All suitability assessment must be in accordance with section 9(5)] to have such access.	**Nil**	
s 9(1)	**A responsible entity must establish and maintain a process or system in the entity's CIRMP to minimise or eliminate the material risk:**		
s 9(1)(c)(i)	Arising from malicious or negligent employees or contractors; and	**Nil**	
s 9(1)(c)(ii)	Arising from the off-boarding process for outgoing employees and contractors.	**Nil**	
s 9(6)	**In deciding to adopt, review or vary a CIRMP, a responsible entity must also have regard to whether the CIRMP:**		
s 9(6)(a)	Lists the entity's critical workers.	**Nil**	
s 9(6)(b)	Describes the personnel risks which could have a relevant impact on the CI asset.	**Nil**	

Supply chain hazards		Chapter 7	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
s 10(1)	**A responsible entity must establish and maintain in the entity's CIRMP a process or system to—as far as it is reasonably practicable to do so – minimise or eliminate the following material risks:**		
s 10(1)(a)(i)	Unauthorised access, interference or exploitation of the asset's supply chain; and	**Nil**	
s 10(1)(a)(ii)	Misuse of privileged access to the asset by any provider in the supply chain; and	**Nil**	
s 10(1)(a)(iii)	Disruption of the asset due to an issue in the supply chain; and	**Nil**	
s 10(1)(a)(iv)	Arising from threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; and	**Nil**	
s 10(1)(a)(v)	Arising from major suppliers; and	**Nil**	
s 10(1)(a)(vi)	Any failure or lowered capacity of other assets and entities in the entity's supply chain	**Nil**	
s 10(1)(b)	As far as it is reasonably practicable to do so—mitigate the relevant impact of a supply chain hazard on the asset	**Nil**	
s 10(2)	**In deciding to adopt, review or vary a CIRMP, a responsible entity to which this enhanced requirement applies must also have regard to whether the CIRMP:**		
s 10(2)(a)	Lists the entity's major suppliers.	**Nil**	
s 10(2)(b)	Describes the supply chain hazards, which could have a relevant impact on the CI asset.	**Nil**	

Physical security hazards and natural hazards		Chapter 8	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
s 11(1)	**A responsible entity must establish and maintain a process or system in the entity's CIRMP:**		
s 11(1)(a)	To identify the physical critical components of the CI asset.	**Nil**	
s 11(1)(b)	As far as it is reasonably practicable to do so—to minimise or eliminate a material risk, and mitigate a relevant impact, of: • a physical security hazard on a physical critical component; and • a natural hazard on the CI asset.	**Nil**	
s 11(1)(c)	To respond to incidents where unauthorised access to a physical critical component occurs.	**Nil**	
s 11(1)(d)	To control access to physical critical components, including restricting access to only those individuals who are critical workers or accompanied visitors.	**Nil**	
s 11(1)(e)	To test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements.	**Nil**	
s 11(2)	**In deciding to adopt, review or vary a CIRMP, a responsible entity must have regard to whether the:**		
s 11(2)(a)	Asset's critical components are described in the CIRMP.	**Nil**	
s 11(2)(b)	Physical security hazards, the occurrence of which could have a relevant impact on a physical critical component, are described in the CIRMP.	**Nil**	
s 11(2)(c)	Security arrangements for the asset are described in the CIRMP.	**Nil**	
s 11(2)(d)	CIRMP describes the natural hazards, the occurrence of which could have a relevant impact on the physical critical component.	**Nil**	

Checklists for enhanced CIRMP

All hazards		Chapter 2	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
S 6, 6A, and 7(1)	**A responsible entity must establish and maintain a process or system in the entity's CIRMP:**		
s 7(1)(a)	To identify the operational context of the CI asset.	**Nil**	
s 7(1)(b)	To identify the material risks to the CI asset.	**Nil**	
s 7(1)(c)	As far as it is reasonably practicable to do so: • to minimise or eliminate the material risks, which may include those mentioned in sections 6 and 6A; and • to mitigate the relevant impact of each hazard on the CI asset.	**Nil**	
s 6(a)	To minimise or eliminate the material risk of a stoppage or major slowd own of the CI asset's function for an unmanageable period.	**Nil**	
s 6(b)	To minimise or eliminate the material risk of a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the CI asset.	**Nil**	
s 6(c)	To minimise or eliminate the material risk of an interference with the CI asset's operational technology or information communication technology essential to the functioning of the asset. *Example A Supervisory Control and Data Acquisition SCADA system.*	**Nil**	
s 6(d)	To minimise or eliminate the material risk of the storage, transmission or processing of sensitive operational information outside Australia, which includes: • layout diagrams; • schematics; • geospatial information; • configuration information; • operational constraints or tolerances information; • data that a reasonable person would consider to be confidential or sensitive about the asset;	**Nil**	
s 6(e)	To minimise or eliminate the material risk of a remote access to operational control or operational monitoring systems of the CI asse	**Nil**	
s 6(f)	To minimise or eliminate the material risk of a impact to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data.	**Nil**	
s 6A(2)(a)	To minimise or eliminate the material risk any impairment of the functions of the CI asset that could prejudice the social stability, economic stability, national security or defence of Australia.	**10 June 2027**	
s 6A(2)(b)	Compromise or impairment of the functions of the CI asset as a result of, or in connection with FOCI.	**10 June 2027**	
s 6A(2)(c)	Offshore or remote access to critical components.	**10 June 2027**	
s 6A(2)(d)	Offshore or remote access to business critical data.	**10 June 2027**	

All hazards		Chapter 2	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
s 7(1)(d)	To review the CIRMP to ensure compliance with section 30AE [*Review of critical infrastructure risk management program]* of the Act.	**Nil**	
s 7(1)(e)	To keep the CIRMP current to ensure it complies with section 30AF [*Update of critical infrastructure risk management program*] of the Act.	**Nil**	
s 7(2)	**In deciding to adopt, review or vary a CIRMP, a responsible entity must have regard to whether the CIRMP:**		
s 7(2)(a)	Describes the outcome of the process or system to identify the operational context.	**Nil**	
s 7(2)(b)	Describes interdependencies between the entity's CI asset and other CI assets.	**Nil**	
s 7(2)(c)	Identifies each position within the entity: • that is responsible for developing and implementing the CIRMP and • that is responsible for reviewing or keeping the CIRMP up to date.	**Nil**	
s 7(2)(d)	Contains the contact details for the positions responsible for the CIRMPs development, implementation, review or maintenance.	**Nil**	
s 7(2)(e)	Contains a risk management methodology.	**Nil**	
s 7(2)(f)	Describes the circumstances in which the entity will review the CIRMP.	**Nil**	

Cyber and Information Security Hazard		Chapter 3	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
s 8(2)	**A responsible entity must establish and maintain a process or system in the CIRMP to—as far as it is reasonably practicable to do so:**		
s 8(2)(a)	Minimise or eliminate any material risk of a cyber and information security hazard occurring.	**Nil**	
s 8(2)(b)	Mitigate the relevant impact of a cyber and information security hazard on the CI asset.	**Nil**	
s 8A(2)	**A responsible entity must establish and maintain a process or system in the entity's CIRMP to—so far as it is reasonably practicable to do so—minimise or eliminate each of the following material risks:**		
s 8A(2)(a)	Failure to patch or update operating or security systems in a timely manner.	**10 June 2027**	
s 8A(2)(b)	Failure to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued.	**10 June 2027**	
s 8A(2)(c)	Deployment or hosting of advanced, novel or emerging technology in a manner that could prejudice the availability, integrity, reliability or confidentiality of the CI asset.	**10 June 2027**	
s 8A(2)(d)	Use of advanced, novel or emerging technology against the asset, in a manner that could prejudice the availability, integrity, reliability or confidentiality of the CI asset.	**10 June 2027**	
s 8(4), (5) and s 8A(3)	**A responsible entity must establish and maintain a process or system in the CIRMP to:**		
s 8(4)(a) s 8(5)	Comply with a framework [or alternative equivalent framework (section 8(5))] contained in a document mentioned in the table in section 8(4) as in force from time to time.	**Nil**	
s 8(4)(b)	Meet any conditions mentioned in the table in section 8(4) for the document.	**Nil**	
s 8A(3)(b)	Comply with a framework contained in a document mentioned in the table at section 8A(3) [or alternative equivalent framework that meets the same security level as a document mentioned in items 2,4, or 5 of that table (section 8A(4))] as in force from time to time [note that the frameworks listed in the table are different to those contained in section 8(4)].	**10 June 2028**	
s 8A(3)(a)	Meet any conditions mentioned in the table at section 8A(3)for the document [note that the conditions listed in the table are different to those contained in section 8(4)].	**10 June 2028**	
Explanatory note – Entities subject to the enhanced CIRMP must comply with a baseline cyber security framework. There is no grace period. They must be compliant with sections 8A(3) or (4) by 10 June 2028			
Explanatory note – As per section 4A(4) to the extent that any inconsistency may arise between a baseline CIRMP requirement and an enhanced CIRMP requirement, the responsible entity must comply with the enhanced CIRMP requirement.			
s 8(6) and s8A(5)	**In deciding to adopt, review or vary a CIRMP, a responsible entity must have regard to whether the CIRMP.**		
s 8(6)	Describes the cyber and information security hazards that could have a relevant impact on the asset.	**Nil**	
s 8A(5)	Contains appropriate measures that minimise or eliminate material risks to the asset including those specified in section 8A(2).	**10 June 2028**	
Explanatory note – As per section 4A(4) to the extent that any inconsistency may arise between a baseline CIRMP requirement and an enhanced CIRMP requirement, the responsible entity must comply with the enhanced CIRMP requirement.			

Credential Compromise Hazard		Chapter 4	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
Explanatory note – as per section 8B(1) – This section [section 8B] only applies if a responsible entity complies with a framework specified under subsection 8A(3) or (4) [cyber security framework] which does not require the implementation of phishing resistant multi-factor authentication.			
s 8B(3), (4) and (5)	**A responsible entity for a CI asset to which this enhanced requirement applies must establish and maintain a process or system in the entity's CIRMP to—so far as it is reasonably practicable to do so:**		
s 8B(3)(a)	Outline the systems or networks where phishing resistant multi-factor authentication is required to authenticate: • access to their organisation's internet connected computers and critical systems • privileged and unprivileged access to critical components, and • remote access to computer applications, systems or services.	**10 June 2028**	
s 8B(3)(b)	• Minimise or eliminate any material risk of a credential compromise hazard occurring.	**10 June 2028**	
s 8B(3)(c)	• Mitigate the relevant impact of the credential compromise hazard on the CI asset.	**10 June 2028**	
s 8B(4)	A responsible entity will be considered to have minimised or eliminated any material risk that the occurrence of a credential compromise hazard could have a relevant impact on the CI asset if they have implemented phishing resistant multi-factor authentication controls in accordance with the below:	**10 June 2028**	
s 8B(5)(a)	Implement phishing resistant multi-factor authentication controls for the systems and networks outlined in paragraph 8B(3)(a); and	**10 June 2028**	
s 8B(5)(b)	Centrally log, monitor and routinely review both successful and unsuccessful multi-factor authentication attempts.	**10 June 2028**	
s 8B(6)	**In deciding to adopt, review or vary a CIRMP, a responsible entity must also have regard to whether the CIRMP:**		
s 8B(6)(a)	Includes a process or system capable of outlining all of the systems and networks where phishing resistant multi-factor authentication is required under section 8B(3)(a).	**10 June 2028**	
s 8B(6)(b)	Describes the credential compromise hazards that could have a relevant impact on the asset.	**10 June 2028**	
s 8B(6)(c)	Contains appropriate measures to minimise or eliminate material risks to the asset.	**10 June 2028**	

Lateral Movement Hazard		Chapter 5	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliance**
s 8C(2), (3), and (4)	**A responsible entity for a CI asset must establish and maintain a process or system in the entity's CIRMP to:**		
s 8C(2)(a)	Identify and maintain an inventory of critical systems and how they are connected with other critical systems and other computers.	**10 June 2028**	
s 8C(2)(b)	Recover and restore critical systems in the event where an incident has had or is having a relevant impact on the asset.	**10 June 2028**	
s 8C(2)(c)	Ensure the continued availability of the asset whilst rebuilding or restoring critical systems.	**10 June 2028**	
s 8C(2)(d)	As far as it is reasonably practicable to do so: • minimise or eliminate any material risk of a lateral movement hazard occurring; and • mitigate the relevant impact of the lateral movement hazard on the CI asset.	**10 June 2028**	
s 8C(3) – (4)	A responsible entity will be considered to have minimised or eliminated any material risk that the occurrence of a lateral movement hazard could have a relevant impact on the CI asset if they have implemented network segregation of critical systems in accordance with the below:	**10 June 2028**	
s 8C(4)(a)	Ensuring critical systems can be segregated as between critical systems, and between critical systems and other computers	**10 June 2028**	
s 8C(4)(b)	Ensuring critical systems can be operationally independent from other internet connected computers and critical systems	**10 June 2028**	
s 8C(4)(c)	Ensuring critical systems can continue to be operational for a period of at least three months while other computers are in a state of restoration or recovery	**10 June 2028**	
s 8C(4)(d)	Implementing logical access controls for network traffic between critical systems, and between critical systems and other computers	**10 June 2028**	
s 8C(4)(e)	Centrally logging, monitoring and routinely reviewing access logs for communication paths between critical systems, and between critical systems and other computers	**10 June 2028**	
s 8C(4)(f)	Implementing principles of least privilege across computers that connect to critical systems	**10 June 2028**	
s 8C(5)	**In deciding to adopt, review or vary a CIRMP, a responsible entity must also have regard to whether the CIRMP:**		
s 8C(5)(a)	Describes the lateral movement hazards that could have a relevant impact on the asset.	**10 June 2028**	
s 8C(5)(b)	Includes a process or system capable of identifying: • critical systems and how they are connected with other critical systems and other computers • methods of recovery and restoration of critical systems where an incident has had or is having a relevant impact on the asset, and methods to ensure the continued availability of the asset whilst rebuilding or restoring critical systems.	**10 June 2028**	
s 8C(5)(c)	Contains appropriate measures to minimise or eliminate material risks to the asset.	**10 June 2028**	

Personnel Hazards		Chapter 6	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliance**
s 9(1)	**A responsible entity must establish and maintain a process or system in the entity's CIRMP:**		
s 9(1)(a)	To identify the entity's critical workers;	**Nil**	
s 9(1)(b)	To permit a critical worker access to critical components of the CI asset only where the critical worker has been assessed to be suitable [suitability assessments may include an AusCheck background check, in which case responsible entities must include an assessment in accordance with section 9(3). All suitability assessment must be in accordance with section 9(5)] to have such access. [There are additional suitability requirements at section 9A(3)-(6) for responsible entities for CI assets to which the enhanced CIRMP applies]	**Nil**	
s 9(1) and 9A(2)	**A responsible entity must establish and maintain a process or system in the entity's CIRMP to minimise or eliminate the material risk:**		
s 9(1)(c)(i)	Arising from malicious or negligent employees or contractors; and	**Nil**	
s 9(1)(c)(ii)	Arising from the off-boarding process for outgoing employees and contractors.	**Nil**	
s 9A(2)(a)	Unauthorised or unsupervised access to critical components.	**10 June 2027**	
s 9A(2)(b)	The compromise or misuse of credentials and privileged access used by individuals to access the CI asset.	**10 June 2027**	
s 9A(2)(c)	Access to the CI asset by persons other than critical workers for the CI asset.	**10 June 2027**	
s 9A(2)(d)	Incoming and outgoing critical workers.	**10 June 2027**	

s 9A(3) – (6)	A responsible entity for a CI asset must establish and maintain a process or system in the entity's CIRMP to:		
s 9A(3)(a)	Permit a critical worker access to critical components only where • the critical worker has been assessed to be suitable in accordance with subsection (4), or • if the critical worker is unable to meet the above requirement – the responsible entity has outlined in their CIRMP the risk associated with the employment of the critical worker and actions taken, or actions that will be taken as soon as reasonably practicable to do so, to minimise or eliminate the risk to the asset.	**10 June 2028**	
s 9A(4)	For the purposes of assessing suitability, a critical worker may only be assessed as suitable if: • they have been the subject of an AusCheck background check, and following that, have been assessed by the responsible entity as suitable, considering the prescribed matters in subsection 9(5); or • The critical worker holds a relevant security clearance at the time the person was identified to be a critical worker.	**10 June 2028**	
s 9A(5)	If a CIRMP permits an AusCheck background check to be conducted for the purposes of paragraph (4)(a), the background check must: • include an assessment of the information outlined in subsection 9(3); • be conducted in accordance with subsection 9(4); and • if the background check relates to a person requiring ongoing access to critical components—be conducted (at minimum) every 5 years.	**10 June 2028**	
s 9A(6)	If the CIRMP permits a critical worker access to critical components where the critical worker has been assessed as suitable by holding a relevant security clearance for the purposes of paragraph (4)(b) [if the worker holds a relevant security clearance], the responsible entity must establish and maintain a process or system in their CIRMP to ensure that, before that clearance lapses or expires, the person has: • undergone a revalidation of their relevant security clearance; or • undergone an AusCheck background check and has been assessed as suitable by the responsible entity considering the matters in subsection 9(5).	**10 June 2028**	
s 9A(3)(b)	Proactively monitor, identify and take action in relation to any developments or changes that may affect the ongoing suitability of a critical worker.	**10 June 2028**	
s 9A(6) and 9A(7)	**In deciding to adopt, review or vary a CIRMP, a responsible entity must also have regard to whether the CIRMP:**		
s 9(6)(a)	Lists the entity's critical workers.	**Nil**	
s 9(6)(b)	Describes the personnel risks, the occurrence of which could have a relevant impact on the CI asset.	**Nil**	
s 9A(7)(a)	Contains appropriate measures that minimise or eliminate material risks to the CI asset including – but not limited to – those specified in section 9A(2).	**10 June 2028**	
s 9A(7)(b)	Includes processes or systems capable of identifying the suitability of workers for the CI asset in accordance with sections 9A(3) and (4).	**10 June 2028**	

Supply chain hazards		Chapter 7	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
s 10(1)	**A responsible entity must establish and maintain in the entity's CIRMP a process or system to—as far as it is reasonably practicable to do so – minimise or eliminate the following material risks:**		
s 10(1)(a)(i)	Unauthorised access, interference or exploitation of the asset's supply chain; and	**Nil**	
s 10(1)(a)(ii)	Misuse of privileged access to the asset by any provider in the supply chain; and	**Nil**	
s 10(1)(a)(iii)	Disruption of the asset due to an issue in the supply chain; and	**Nil**	
s 10(1)(a)(iv)	Arising from threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; and	**Nil**	
s 10(1)(a)(v)	Arising from major suppliers; and	**Nil**	
s 10(1)(a)(vi)	Any failure or lowered capacity of other assets and entities in the entity's supply chain	**Nil**	
s 10(1)(b)	As far as it is reasonably practicable to do so—mitigate the relevant impact of a supply chain hazard on the asset.	**Nil**	

s 10A(2) and (3)	Supply Chain mapping		
s 10A(2)	A responsible entity of a CI asset must establish and maintain a system or process in the entity's CIRMP to map their supply chain for major suppliers and critical components across their supply chain. The CIRMP must:	**10 June 2028**	
s 10A(3)(a)	Identify risks in the entity's supply chain that may affect the availability, integrity, reliability or confidentiality of critical components or compromise business critical data.	**10 June 2028**	
s 10A(3)(b)	Identify the maximum acceptable outage for the CI asset or any of its critical components arising from the disruption to the entity's supply chain.	**10 June 2028**	
s 10A(3)(c)	As far as is reasonably practicable to do so—include measures to minimise or eliminate those risks, or mitigate the impact of an outage that exceeds the maximum acceptable outage.	**10 June 2028**	
s 10A(4)	A responsible entity of a CI asset must establish and maintain a system or process in the entity's CIRMP to assess the risks associated with an existing or proposed major supplier for the CI asset. For each existing or proposed major supplier, the CIRMP must:	**10 June 2028**	
s 10A(5)(a)	In relation to FOCI risks—legislative or other legal requirements to which the supplier is subject to.	**10 June 2028**	
s 10A(5)(b)	Restrictions, sanctions or other impediments affecting the jurisdiction to which the entity may be subject to.	**10 June 2028**	
s 10A(5)(c)	The access, influence and control the supplier has over the CI asset in connection with the product or service the supplier provides.	**10 June 2028**	
s 10A(5)(d)	Regarding matters raised in paragraphs (a), (b) and (c)—The extent to which these matters together may present a material risk for the CI asset, or could exceed a maximum acceptable outage of the service or product provided by the supplier.	**10 June 2028**	
s 10A(5)(e)	As far as reasonably practicable to do so—steps to minimise or eliminate material risks and mitigate the relevant impact of the hazard on the CI asset.	**10 June 2028**	
s 10(2) and 10A(6)	**In deciding to adopt, review or vary a CIRMP, a responsible entity to which this enhanced requirement applies must also have regard to whether the CIRMP:**		
s 10(2)(a)	Lists the entity's major suppliers.	**Nil**	
s 10(2)(b)	Describes the supply chain hazards, which could have a relevant impact on the CI asset.	**Nil**	
s 10A(6)(a)	Includes a process or system capable of identifying the matters in sections 10A(3)(a) - (c).	**10 June 2028**	
s 10A(6)(b)	Includes a process or system capable of identifying risks the matters in sections 10A(5)(a) - (e).	**10 June 2028**	

Physical security hazards and natural hazards		Chapter 8	
CIRMP Rules	**CIRMP requirements**	**Grace period ends**	**Compliant**
s 11(1) and 11A(1)	**A responsible entity must establish and maintain a process or system in the entity's CIRMP:**		
s 11(1)(a)	To identify the physical critical components of the CI asset.	**Nil**	
s 11(1)(b)	As far as it is reasonably practicable to do so—to minimise or eliminate a material risk, and mitigate a relevant impact, of: • a physical security hazard on a physical critical component; and • a natural hazard on the CI asset.	**Nil**	
s 11(1)(c)	To respond to incidents where unauthorised access to a physical critical component occurs.	**Nil**	
s 11(1)(d)	To control access to physical critical components, including restricting access to only those individuals who are critical workers or accompanied visitors.	**Nil**	
s 11(1)(e)	To test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements.	**Nil**	
s 11A(1)(a)	Centrally manage physical security and natural hazards. Including outlining:	**10 June 2028**	
S 11A(2)	• the location, ownership, and nature of the site upon which their asset is located • the critical components of the CI asset • areas within the asset that hold business critical data or contain critical components including critical systems	**10 June 2028**	
s 11A(1)(b)	As far as it is reasonably practicable to do so—outline and consider the physical security consequences arising from the occurrence of all hazards, including cyber and information security hazards, credential compromise hazards, lateral movement hazards, other physical and natural hazards, personnel hazards and supply chain hazards. For the purpose of the above – the responsible entity must, as far as reasonably practicable, consider and outline the following:	**10 June 2028**	
s 11A(3)(a)	Any physical access controls to the CI asset for workers, official visitors, and the public, including but not limited to: • access controls for critical components and critical systems to restrict access to critical workers or accompanied visitors; • maintaining surveillance and security alarm systems, such that critical components and critical systems are subject to continuous monitoring; • specific protective security measures for business hours and out-of-hours.	**10 June 2028**	
s 11A(3)(b)	Other security measures that increase the ability to deter, detect, delay, respond to and recover from a breach in security for all critical components.	**10 June 2028**	
s 11A(3)(c)	Mitigation and response measures to be taken where a physical security incident or a physical security consequence has been detected.	**10 June 2028**	

s 11(2) and 11A(4)	In deciding to adopt, review or vary a CIRMP, a responsible entity must have regard to whether the:		
s 11(2)(a)	Asset's critical components are described in the CIRMP.	**Nil**	
s 11(2)(b)	Physical security hazards, the occurrence of which could have a relevant impact on a physical critical component, are described in the CIRMP.	**Nil**	
s 11(2)(c)	Security arrangements for the asset are described in the CIRMP.	**Nil**	
s 11(2)(d)	CIRMP describes the natural hazards, the occurrence of which could have a relevant impact on the physical critical component.	**Nil**	
s 11A(4)	Contains systems or processes capable of identifying the matters set out in sections 11A(1) - (3).	**10 June 2028**	

Attachment D – Obligations tables

These tables bring together the obligations outlined throughout this guidance in one location. They are intended to help responsible entities identify the requirements that apply to CI assets subject to the baseline or enhanced CIRMP or TSRMP requirements.

The tables are organised by hazard category and provide the relevant legislative references for each obligation. They should be read together with the relevant chapters of this guidance, which provide further explanation and practical information about meeting the obligations.



All hazards obligation table

All hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Establish and maintain a process or system to identify the operational context of the CI asset.	s 7(1)(a)	s 7(1)(a)	s 9(a)
Establish and maintain a process or system to identify the material risks to the CI asset.	s 7(1)(b)	s 7(1)(b)	s 9(b)
Establish and maintain a process or system to – as far as it is reasonably practicable to do so – minimise or eliminate the material risks and mitigate the relevant impact of each hazard on the CI asset. The material risks may include: (a) A stoppage or major slowdown of the CI asset's function for an unmanageable period (b) A substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the CI asset Example - The position, navigation and timing systems affecting provision of service or functioning of the asset. (c) An interference with the CI asset's operational technology or information communication technology essential to the functioning of the asset Example - A Supervisory Control and Data Acquisition (SCADA) system. (d) The storage, transmission or processing of sensitive operational information outside Australia, which includes: (i) Layout diagrams (ii) Schematics (iii) Geospatial information (iv) Configuration information (v) Operational constraints or tolerances information (vi) Data that a reasonable person would consider to be confidential or sensitive about the asset (e) Remote access to operational control or operational monitoring systems of the CI asset (f) Impact to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data.	s 6 s 7(1)(c)	s 6 s 7(1)(c)	s 8 s 9(c)
Establish and maintain a process or system to – as far as it is reasonably practicable to do so – minimise or eliminate the additional material risks specified in subsection 6A(2) of the CIRMP Rules. The following specified risks are additional material risks: (a) any impairment of the CI asset's functions that could prejudice the social stability, economic stability, national security or defence of Australia; (b) compromise or impairment of the functions of the CI asset as a result of, or in connection with FOCI; (c) offshore or remote access to critical components; and (d) offshore or remote access to business critical data.		s 6A(1) s 6A(2)	

Cyber and information hazard obligation table

Cyber and information security hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
A responsible entity for a CI asset must establish and maintain a process or system to – so far as reasonably practicable to do so – minimise or eliminate any material risk of a cyber and information security hazard occurring and mitigate the relevant impact of a cyber and information security hazard on the CI asset.	s 8(2)	s 8(2)	s 11(2)
A responsible entity for a CI asset must establish and maintain a process or system to comply with a framework contained in a document specified in the CIRMP (and if applicable – the TSRMP) Rules, and meet any relevant conditions mentioned in the Rules for that document. The responsible entity must otherwise establish and maintain a process or system in the entity's CIRMP to comply with a framework that is equivalent to a framework contained in a document specified in the CIRMP (and if applicable – the TSRMP) Rules, including any relevant conditions mentioned in the Rules for that document.	s 8(4) s 8(5)	s 8A(3) s 8A(4)	s 11(3) s 11(4) s 11(5)
A responsible entity for a CI asset subject to the enhanced CIRMP must establish and maintain a process or system in the entity's CIRMP to – so far as it is reasonably practicable to do so – minimise or eliminate each of the following material risks: (a) Failure to patch or update operating or security systems in a timely manner; (b) Failure to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued; (c) Deployment or hosting of advanced, novel or emerging technologies that could prejudice the availability, integrity, reliability or confidentiality of the CI asset; and (d) Use of advanced, novel or emerging technologies against the asset, in a manner that could prejudice the availability, integrity, reliability or confidentiality of the CI asset.		s 8A(2)	

Credential compromise hazard obligation table

Credential compromise hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Responsible entities must establish and maintain a process or system in their CIRMP to — so far as is reasonably practicable to do so — outline the systems or networks where phishing resistant multi-factor authentication (MFA) is required to authenticate: (i) access to their organisation's internet connected computers and critical systems; (ii) privileged and unprivileged access to critical components; (iii) remote access to computer applications, systems or services.		s 8B(3)(a)	
Responsible entities must establish and maintain a process or systemin their CIRMP to — so far as it is reasonably practicable to do so — to: (b) minimise or eliminate any material risk of a credential compromise hazard occurring; and (c) mitigate the relevant impact of the credential compromise hazard on the CI asset.		s 8B(3)(b) s 8B(3)(c)	
If a responsible entity implements the MFA controls in section 8B(5)(a) and section 8B(5)(b) they are taken to have acquitted the obligation to minimise or eliminate any material risk that a credential compromise hazard could have a relevant impact on the asset. The MFA controls in sections 8B(5)(a) and (b) are as follows: (a) implement phishing resistant MFA controls for the systems and networks outlined in s 8B(3)(a); and (b) centrally log, monitor and routinely review both successful and unsuccessful MFA attempts.		s 8B(4) s 8B(5)	

Lateral movement hazard obligation table

Lateral movement hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Responsible entities must establish and maintain a process or system to identify and maintain an inventory of critical systems and how they are connected with other critical systems and other computers.		s 8C(2)(a)	
Responsible entities must establish and maintain a process or system to recover and restore critical systems in the event where an incident has had or is having a relevant impact on the asset.		s 8C(2)(b)	
Responsible entities must establish and maintain a process or system to ensure the continued availability of the asset whilst rebuilding or restoring critical systems.		s 8C(2)(c)	
Responsible entities must establish and maintain a process or system to – as far as reasonably practicable to do so: (i) minimise or eliminate any material risk of a lateral movement hazard occurring; and (ii) mitigate the relevant impact of the lateral movement hazard on the CI asset.		s 8C(2)(d)	
If a responsible entity implements the network segregation in section 8C(4) they are taken to have acquitted the obligation to minimise or eliminate the material risks that a lateral movement hazard could have a relevant impact on the CI asset. The network segregation in section 8C(4) are as follows: (a) ensuring critical systems can be segregated as between critical systems, and between critical systems and other computers; (b) ensuring critical systems can be operationally independent from other internet connected computers and critical systems; (c) ensuring critical systems can continue to be operational for a period of at least three months while other computers are in a state of restoration or recovery; (d) implementing logical access controls for network traffic between critical systems, and between critical systems and other computers; (e) centrally logging, monitoring and routinely reviewing access logs for communication paths between critical systems, and between critical systems and other computers; and (f) implementing principles of least privilege across computers that connect to critical systems.		s 8C(4)	

Personnel hazard obligation table

Personnel hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Responsible entities must establish and maintain a process or system in the entity's CIRMP to identify the entity's critical workers.	s 9(1)(a)	s 9(1)(a)	s 12(1)(a)
Responsible entities must establish and maintain a process or system in the entity's CIRMP to permit a critical worker access to critical components of the CI asset only where the critical worker has been assessed to be suitable to have such access.	s 9(1)(b)	s 9(1)(b)	s 12(1)(b)
Responsible entities must establish and maintain a process or system in the entity's CIRMP, to – as far as it is reasonably practicable to do so – minimise or eliminate the material risks: (i) arising from malicious or negligent employees or contractors; and (ii) arising from the off-boarding processes for outgoing employees and contractors.	s 9(1)(c)	s 9(1)(c)	s 12(1)(c)
Responsible entities must establish and maintain a process or system in the entity's CIRMP to minimise or eliminate the material risks associated with: (a) unauthorised or unsupervised access to critical components; (b) the compromise or misuse of credentials and privileged access used by individuals to access the CI asset; (c) access to the CI asset by persons other than critical workers for the CI asset; and (d) incoming and outgoing critical workers.		s 9A (2)	
Responsible entities must establish and maintain a process or system in the entity's CIRMP to permit a critical worker access to critical components only where they have been assessed to be suitable (i) the critical worker has been assessed to be suitable in accordance with subsection 9A(4) [see information contained at **6.2.5**]; or (ii) if the critical worker is unable to meet the requirements outlined in subsection 9A(4) – the responsible entity has outlined in their CIRMP the risk associated with the employment of the critical worker and actions taken, or action that will be taken as soon as reasonably practicable to do so, to minimize or eliminate the risk to the asset.		s 9A(3)(a)	
Responsible entities must establish and maintain a process or system in the entity's CIRMP to proactively monitor, identify and take action in relation to any developments or changes that may affect the ongoing suitability of a critical worker.		s 9A(3)(b)	

Supply chain hazard obligation table

Supply chain hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Responsible entities must establish and maintain a process or system in the entity's CIRMP to - as far as it reasonably practicable to do so - minimise or eliminate the following material risks: (i) Unauthorised access, interference or exploitation of the asset's supply chain; (ii) Misuse of privileged access to the asset by any provider in the supply chain; (iii) Disruption of the asset due to an issue in the supply chain; (iv) Arising from threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; (v) Arising from major suppliers; and (vi) Any failure of lowered capacity of other assets and entity's supply chain. The responsible entity must also - as far as it reasonably practicable to do so - mitigate the relevant impact of a supply chain hazard on the asset	s 10(1)	s 10(1)	s 14(1)
Responsible entities must establish and maintain a system or process in the entity's CIRMP to map their supply chain for major suppliers and critical systems across their supply chains. The entity's CIRMP must: identify risks in the entity's supply chain that may affect the availability, integrity, reliability or confidentiality of critical components or compromise business critical data; and identify the maximum acceptable outage for the CI asset or any of its critical components arising from the disruption to the entity's supply chain; and as far as is reasonably practicable to do so—include measures to minimise or eliminate those risks, or mitigate the impact of an outage that exceeds the maximum acceptable outage.		s 10A(2) s 10A(3)	
Responsible entities must establish and maintain a system or process in the entity's CIRMP to assess the risks associated with an existing or proposed major supplier for the CI asset. The system or process must identify, for each existing or proposed major supplier: in relation to foreign ownership, control or influence (FOCI) risks— legislative or other legal requirements to which the supplier is subject to; and restrictions, sanctions or other impediments affecting the jurisdiction to which the entity may be subject to; and the access, influence and control the supplier has over the CI asset in connection with the product or service the supplier provides; and the extent to which the matters in paragraphs (a), (b) and (c) together may present a material risk for the CI asset, or could exceed a maximum acceptable outage of the service or product provided by the supplier; and as far as reasonably practicable to do so— steps to minimise or eliminate material risks and mitigate the relevant impact of the hazard on the CI asset.		s 10A(4) s 10A(5)	

Physical security and natural hazard obligation table

Physical security hazard and natural hazard obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
Responsible entities must establish and maintain a process or system in their CIRMP to identify the physical critical components of the CI asset.	S 11(1)(a)	s 11(1)(a)	S 15(1)(a)
Responsible entities must establish and maintain a process or system in their CIRMP to – as far as it is reasonably practicable to do so – minimise or eliminate a material risk and mitigate a relevant impact of: (i) a physical security hazard on a physical critical component; and (ii) a natural hazard on the CI asset.	s 11(1)(b)	s 11(1)(b)	s 15(1)(b)
Responsible entities must establish and maintain a process or system in their CIRMP to respond to incidents where unauthorised access to a physical critical component occur.	s 11(1)(c)	s 11(1)(c)	s 15(1)(c)
Responsible entities must establish and maintain a process or system in their CIRMP to control access to physical critical components, including restricting access to only those individuals who are critical workers or accompanied visitor.	s 11(1)(d)	s 11(1)(d)	s 15(1)(d)
Responsible entities must establish and maintain a process or system in their CIRMP to test that security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements.	s 11(1)(e)	s 11(1)(e)	s 15(1)(e)
Responsible entities must establish and maintain a process or system in their CIRMP to centrally manage physical security and natural hazards. For the purposes of this obligation the responsible entity must outline: (a) the location, ownership, and nature of the site upon which their asset is located; and (b) the critical components of the CI asset; and (c) areas within the asset that hold business critical data or contain critical components including critical systems.		11A(1)(a) 11A(2)	

Maintaining your CIRMP obligation table

Maintaining the CIRMP and annual reporting obligations	CIRMP Rules		TSRMP Rules
	Baseline	Enhanced	
The responsible entity must establish and maintain a process or system in the entity's CIRMP to review the CIRMP to ensure compliance with section 30AE of the Act.	s 7(1)(d)	s 7(1)(d)	s 9(d)
The responsible entity must establish and maintain a process or system in the entity's CIRMP to keep the CIRMP current to ensure it complies with section 30AF of the Act	s 7(1)(e)	s 7(1)(e)	s 9(e)
	SOCI Act		
A responsible entity must have regard to certain matters in deciding whether to adopt a CIRMP, and when reviewing or varying their CIRMP.	30AKA	30AKA	30AKA
A responsible entity must give an annual report relating to its critical infrastructure risk management program. If the entity has a board, council or other governing body, the annual report must be approved by the board, council or other governing body.	30AG	30AG	30AG
A responsible entity for a critical infrastructure asset that is exempt from Part 2A of the SOCI Act (pursuant to sections 30AB(4)-(6) of the SOCI Act) must give an annual report in accordance with Part 2AA of the Act.	30AQ	30AQ	30AQ

Attachment E – CIRMP entry examples

The guidance provides examples of hazards and the assessment a responsible entity may record to determine whether the hazard is a material risk and the controls in place to manage the risk and the impact of the eventuation of the risk. This document collates all worked examples.

The examples are illustrative only. They are not templates that responsible entities are required to follow, and completing an entry in this format does not, by itself, demonstrate compliance with the CIRMP obligations.

Responsible entities should adapt their approach to the operational context, risk environment and circumstances of each CI asset. The hazards, assessments, controls, owners, timeframes and supporting material included in these examples should not be treated as applying to every asset.



All hazard CIRMP entry example

The below example demonstrates how unauthorised or unmanaged offshore access to critical systems could be captured in an entity's CIRMP.

Field	Example Response
Hazard	Unauthorised or unmanaged offshore access to critical systems
Asset(s) / Site	Network Operations Centre (NOC) – Site B (coordinates delivery of essential services, including monitoring and management systems
Scenario	An offshore service provider is granted access to maintain operational systems. Access controls, monitoring, or contractual restrictions are insufficiently defined or enforced, resulting in elevated, persistent, or inappropriate access beyond operational need.
Why this is material	Offshore access can introduce exposure to risk through external access to systems or data access outside direct operational oversight.
Relevant impact mapping	**Integrity:** unauthorised changes to system configuration, patching, or operational processes through offshore access pathways. **Confidentiality:** exposure of sensitive operational information (system architecture, credentials, incident data) through offshore access.
Evidence supporting likelihood	• Offshore access arrangements documented, including systems accessed and access methods (Completed — Mar 2026). • Access logs and monitoring reports identify frequency and scope of remote sessions (Ongoing review — from Jan 2026). • Internal audit findings identify gaps in access governance, monitoring, or third-party controls (In progress — due Aug 2026).
Key dependencies / interdependencies *(Include here the cascading impact that may result from the realisation of the hazards)*	• Offshore service providers or remote personnel supporting monitoring, maintenance, or incident response. • Identity and access management systems controlling authentication and permissions. • Network architecture enabling remote connectivity (VPNs, gateways, remote access platforms).
Controls — Preparedness	• Defined process for approving, provisioning, and reviewing offshore or remote access (Implemented — Mar 2026). • Risk assessment process applied prior to granting offshore or remote access (Implemented — May 2026).
Controls — Prevent / minimise likelihood	• Restrict offshore or remote access to approved methods (such as managed VPN, secure gateway); prohibit uncontrolled access pathways (Implemented — Jan 2026). • Enforce least-privilege access, time-bound access, and individual user accounts; prohibit shared credentials (Implemented — Jan 2026). • Require multi-factor authentication and device security controls for offshore or remote connections (Implemented — Feb 2026). • Implement session monitoring, logging, and routine review of offshore or remote access activity (Implemented — Jan 2026). • Define contractual controls for third-party offshore access where applicable, including audit rights and security requirements (In progress — Sep 2026).
Controls — Impact mitigation	• Segregate critical systems and limit offshore or remote access to controlled environments where feasible. • Maintain real-time monitoring and alerting for anomalous offshore access behaviour.

	• Maintain incident response procedures specific to offshore or remote access compromise scenarios. • Enable rapid revocation of access (accounts, sessions, credentials) in response to suspected compromise.
Owners / status / timeframes	• Offshore and remote access governance — Head of Cyber Security (implemented, quarterly review) • Third-party access controls — Vendor Management Lead (in progress; Sep 2026). • Monitoring and logging — Security Operations Centre Lead (implemented; uplift Oct 2026).
Residual risk and acceptance	Residual risk assessed as medium due to continued reliance on offshore access pathways and associated visibility and control limitations. Risk accepted by Risk Committee (Jun 2026), subject to ongoing monitoring, periodic access reviews, and continued uplift of access assurance controls.
Review cadence / triggers	Review annually and trigger review after: • onboarding or offboarding of offshore providers or remote users with system access • changes to remote access architecture or authentication methods • significant cyber security incidents involving offshore or remote access pathways • material changes to service delivery arrangements or operating environment
Supporting material	• Offshore and remote access policy and procedures • Third-party risk assessments and contractual agreements (where applicable) • Access control and identity management documentation • Remote access logs and monitoring reports • Incident response plans and scenario exercise outputs

Cyber and information hazard CIRMP entry example

This below example demonstrates how a failure or misuse of an artificial intelligence (AI) enabled decision support capability could be captured in an entity's CIRMP.

Field	Example Response
Hazard	Failure or misuse of an artificial intelligence (AI) enabled decision support capability.
Asset(s) / Site	Primary Operations Centre – Site A. An AI-enabled Operations Decision Support Tool (ODST) is used by operational and technical support staff to analyse operational information and support time-critical decisions. The tool provides recommendations but does not take automatic operational action.
Scenario	An AI-enabled decision support tool provides incorrect recommendations, becomes unavailable during operations, or is misused following a cyber compromise. This affects the ability of staff to make timely and informed operational decisions.
Why this is material	The system supports important operational decisions and provides visibility over operational information. Errors, outages or misuse may disrupt operations, delay restoration or expose sensitive operational information.
Relevant impact mapping	**Availability:** disruption to operational decision-making and service delivery. **Integrity:** incorrect or manipulated recommendations may affect operational decisions and actions. **Confidentiality:** unauthorised access to sensitive operational information.
Evidence supporting likelihood	• ODST dependency mapping identifying the teams, systems and operational scenarios that rely on the tool. • Testing and performance records for recommendations, including identified errors and occasions where staff overrode the tool. • Vendor assurance material covering model updates, access, hosting, data handling and support arrangements.
Key dependencies / interdependencies *(Include here the cascading impact that may result from the realisation of the hazards)*	• Reliable operational data feeds and integrations used to generate recommendations. • Identity, authentication and remote-access services used by operational staff and vendor support personnel. • Operational staff who validate recommendations and maintain situational awareness. • Incorrect outputs or loss of the tool could delay decisions and create cascading impacts across dependent operational functions.
Controls — Preparedness	• Maintain incident playbooks for incorrect recommendations, suspected manipulation, tool outage, credential compromise and vendor incidents. • Maintain documented decision checks and manual operating procedures.
Controls — Prevent / minimise likelihood	• Operate ODST in advisory mode, with no automatic operational actions, until reliability and assurance requirements are met. • Monitor for unusual access, unexpected recommendation patterns and changes in system behaviour. • Apply strong authentication, least privilege and controlled remote access for operational and vendor accounts.
Controls — Impact mitigation	• Require staff to validate AI recommendations against documented checks before acting. • Maintain a clear process to disable ODST and switch to manual procedures. • Revoke affected access, isolate compromised systems and preserve relevant logs following suspected misuse.
Owners / status / timeframes	• ODST integration and configuration control — Operations Systems Manager (In progress; Dec 2026). • Identity, access and monitoring controls — Cyber Security Lead (Implemented; quarterly review).

	• Operational decision checks and manual procedures — Operations Manager, Site A (Implemented; next exercise Nov 2026).
Residual risk and acceptance	Residual risk assessed as medium due to evolving AI-related threats, dependence on vendor support and data feeds, and the potential for plausible but incorrect recommendations. Accepted by the Risk Committee (May 2026), subject to completion of system separation and vendor assurance actions and continued human validation of recommendations.
Review cadence / triggers	Review annually as part of the CIRMP cycle and quarterly during rollout. Trigger review after: • a significant ODST, model, data-source or integration update • a change to the vendor, hosting location, support model or access arrangements • an incorrect recommendation, outage, cyber incident or near miss • evidence of unusual access, manipulation or unexpected system behaviour
Supporting material	• ODST architecture, dependency and data-flow documentation • Documented operational decision checks and manual procedures • Exercise plans, after-action reports and improvement actions • Monitoring rules, incident playbooks and escalation contacts

Credential compromise hazard CIRMP entry example

The below example demonstrates how the hazard of compromise or misuse of credentials could be reflected in an entity's CIRMP.

Field	Example Response
Hazard	Compromise and misuse of credentials used to access internet-connected systems and remote access services.
Asset(s) / Site	Corporate network and remote access gateway supporting access to critical systems used to monitor and manage essential services.
Scenario	Credentials used to authenticate remote access to systems are obtained by a malicious actor through a phishing attack. The actor uses the compromised credentials to gain unauthorised access to internet-connected systems and critical components via remote access pathways.
Why this is material	• Unauthorised access using valid credentials may allow malicious activity to appear legitimate and avoid detection. • Access via remote authentication pathways may enable interaction with critical systems and components, increasing the risk of disruption or manipulation of services.
Relevant impact mapping	**Availability:** disruption or degradation of services due to unauthorised system actions. **Integrity:** unauthorised changes to configurations, processes, or operational data. **Confidentiality**: unauthorised access to sensitive operational or system information.
Evidence supporting likelihood	• Industry reporting identifying credential-based attacks (phishing and credential reuse) as a common initial access vector. • Logs indicating repeated failed authentication attempts across remote access services. • Prior security assessments identifying gaps in authentication controls or credential management practices.
Key dependencies / interdependencies (Include here the cascading impact that may result from the realisation of the risk)	Dependent on secure authentication and access control across: • Remote access services and gateways. • Identity and authentication systems. • Systems supporting monitoring and management of critical components. • Internet-connected services and infrastructure.
Controls — Preparedness	• Implementation of authentication controls (including phishing resistant MFA) for remote and internet-facing access. • Processes for identifying systems requiring strong authentication controls. • Playbooks for responding to credential compromise (credential reset, investigation).
Controls — Prevent / minimise likelihood	• Limiting access permissions associated with credentials (least privilege). • Secure management of credentials, including storage, rotation, and revocation.
Controls — Impact mitigation	• Rapid revocation and reset of compromised credentials. • Monitoring and detection of anomalous authentication activity. • Isolation of affected systems or accounts where unauthorised access is identified.
Owners / status / timeframes	Authentication controls implementation — Security Lead — In progress; Dec 2026. Monitoring and logging improvements — Security Operations Lead — Planned; Oct 2026.

Residual risk and acceptance	Residual risk assessed as medium due to ongoing exposure to credential-based attacks targeting internet-facing systems. Risk accepted by Risk Committee (Jun 2026).
Review cadence / triggers	Formal review annually as part of CIRMP review. Trigger review after: • any suspected or confirmed credential compromise event • significant changes to authentication systems or remote access architecture • changes in threat level due to imminent or actual crisis/conflict.
Supporting material	• Authentication and access control policies • Authentication logs and monitoring reports • Credential lifecycle management procedures

Lateral movement hazard CIRMP entry example

Field	Example Response
Hazard	Unauthorised movement between connected systems following an initial compromise, resulting in disruption across critical systems.
Asset(s) / Site	Operational network supporting control systems for essential service delivery. Includes multiple interconnected critical systems and supporting IT infrastructure.
Scenario	An attacker gains access to a non-critical system connected to the corporate IT environment. Due to inadequate segregation and unrestricted communication pathways, the attacker moves between systems and accesses connected critical systems. The attacker accesses multiple systems using existing trust relationships and communication pathways.
Why this is material	Lateral movement between systems may allow a compromise affecting one system to spread across multiple systems within the CI asset. Movement across systems may allow unauthorised activity to persist undetected and increase the scale and impact of an incident.
Relevant impact mapping	**Availability:** disruption to service delivery due to multiple systems being affected. **Integrity:** unauthorised modification of system configurations or operational processes. **Confidentiality:** unauthorised access to sensitive system or operational information. **Reliability:** degradation in system performance and reduced confidence in system outputs.
Evidence supporting likelihood	Prior security reviews identifying limited segregation between IT and OT systems. Observed system architectures with broad or unnecessary communication pathways. Intelligence reports indicating prepositioning in critical infrastructure is a relevant risk.
Key dependencies / interdependencies ***(Include here the cascading impact that may result from the realisation of the hazards)***	Dependent on connectivity between: • critical systems supporting essential operations. • corporate IT networks and supporting systems. • shared services and infrastructure (authentication, monitoring or data services).
Controls — Preparedness	• Identification and mapping of system connections and dependencies. • Playbooks for responding to incidents involving multiple compromised systems.
Controls — Prevent / minimise likelihood	• Restricting communication pathways between systems to only what is operationally required. • Applying network segregation between critical systems and other environments. • Limiting system-to-system access through least privilege principles.
Controls — Impact mitigation	• Isolating affected systems to prevent further spread of compromise. • Monitoring system communication to detect anomalous behaviour. • Sequencing recovery of systems based on dependencies and criticality.
Owners / status / timeframes	Network architecture review — Engineering Lead — In progress; Nov 2026. • Segregation controls uplift — Security Team — Planned; Jan 2027.
Residual risk and acceptance	Residual risk assessed as medium due to system complexity and interdependencies. Risk accepted by Risk Committee (Jun 2026).
Review cadence / triggers	• Formal review at 24 months as part of CIRMP review. Trigger review after: • any incident involving system-to-system propagation. • significant changes to system architecture or connectivity. • identification of new interdependencies or access pathways. • in the event of a notable increase of threat level.
Supporting material	• Network segmentation design documentation. • Monitoring and logging reports. • Incident response and recovery procedures.

Personnel hazard CIRMP entry example

The below example could be how official overseas travel by a critical worker with their work issued devices could be captured in an entity's CIRMP.

Field	Example Response
Hazard	Official overseas travel by a critical worker with their work issued devices.
Asset(s) / Site	Network Operations Centre (NOC) – **Site B** (coordinates delivery of the essential services). Includes access to key systems used to monitor and manage the service.
Scenario	A critical worker travels overseas and retains remote access to systems used to monitor and manage the service. The worker is targeted (such as through social engineering or device compromise) and credentials that allow access to systems are compromised.
Why this is material	▪ Compromise of a critical worker (or their device/credentials) can enable malicious activity that appears "legitimate" and is harder to detect. ▪ Malicious actors may use compromised devices or credentials to disrupt the proper function of the CI asset. ▪ Access to the credentials may impact Site B which contains systems/areas where interference can cause extended outages and broader downstream impacts.
Relevant impact mapping	**Availability:** service interruption or slowdown due to unauthorised actions. **Integrity:** unauthorised configuration changes or operational actions taken using compromised credentials or under coercion. **Confidentiality:** unauthorised access to sensitive operational information.
Evidence supporting likelihood	▪ Country information available on Smartraveller.gov.au (Reviewed — Mar 2026) ▪ Prior security review identified inconsistent travel notification and variable controls for overseas access (Reviewed — Jan 2026). ▪ Near miss: unusual overseas login attempt during prior travel period (Reviewed — Nov 2025)
Key dependencies / interdependencies **(Include here the cascading impact that may result from the realisation of the hazards)**	Dependent on availability, integrity, and confidentiality of systems in Site B: ▪ Corporate network. ▪ Surveillance and monitoring of critical components. ▪ Remote access to critical componentry. ▪ As a result of impact, critical systems must operate independently until the responsible team can undertake recovery and restoration of the compromised system.
Controls — Preparedness	▪ Travel policy with clear before / during / after travel requirements for critical workers, including declaration and briefings for higher-risk travel. ▪ Playbook for suspected travel-related compromise that includes containment steps, credential resets, device screening, and escalation. ▪ Tabletop exercise: "overseas travel + suspected compromise + operational disruption" (Scheduled — Aug 2026).
Controls — Prevent / minimise likelihood	▪ Limit systems access while overseas to the minimum required (risk- and role-based) and apply stronger sign-in controls for remote/privileged access. ▪ Pre-travel briefings for higher-risk travel. ▪ Avoid taking devices that provide direct access to sensitive systems for higher-risk destinations.
Controls — Impact mitigation	▪ Rapid containment: disable accounts/badges immediately when suspicious activity is detected.

	▪ Post-travel controls: ICT screening before reconnecting devices to corporate systems where required by policy.
Owners / status / timeframes	▪ Travel declaration + briefing process — Security Lead — Implemented; refresh annually. ▪ Monitoring/log review — Security Operations Lead — In progress; Sep 2026. ▪ Post-travel screening workflow — ICT Operations Lead — Planned; Oct 2026.
Residual risk and acceptance	▪ Residual risk assessed as medium due to reliance unavoidable travel requirements for specialist roles. ▪ Risk acceptance approved by the Risk Committee (Jun 2026).
Review cadence / triggers	Formal review annually as part of CIRMP review. Trigger review after: ▪ Any suspected compromise, coercion attempt, or travel-related security incident or near miss. ▪ Significant change to remote access arrangements or overseas travel profile. ▪ Audit findings indicating gaps in travel declaration, briefing, monitoring or post-travel controls.
Supporting material	▪ Travel policy and evidence of completion (briefings, declarations). ▪ List of critical workers with travel notification records.

Supply chain hazard CIRMP entry example

The below example could be how a sub-standard or counterfeit component introduced through the supply chain is captured in an entity's CIRMP.

Field	Example Response
Hazard	Sub-standard or counterfeit component introduced through the supply chain causes equipment failure or degraded performance, disrupting the proper function of the CI asset.
Asset(s) / Site	Primary Operations Centre – Site A. The asset relies on specialist replacement components for operational equipment. Some components have long lead times and cannot be readily substituted during urgent maintenance.
Scenario	A replacement component is sourced through an approved supplier or distributor under time pressure during urgent maintenance. The component appears genuine but is sub-standard or counterfeit. After installation, the component fails or performs below specification, affecting the equipment and delaying restoration while a verified replacement is sourced.
Why this is material	The component supports equipment required for the proper function of the CI asset. Failure or degraded performance could disrupt operations and extend restoration beyond the maximum tolerable outage, particularly where verified replacement parts and specialist support are not immediately available.
Relevant impact mapping	**Integrity:** a compromised component undermines system integrity and may invalidate assurance about the condition or performance of the equipment. **Reliability:** sub-standard performance increases the likelihood of repeat failures and unreliable operation. **Availability:** equipment failure and delayed replacement may extend disruption to the asset's functions.
Evidence supporting likelihood	▪ Previous component failures, warranty claims and maintenance records, including failures shortly after installation. ▪ Manufacturer and supplier alerts about counterfeit or non-conforming components. ▪ Quality inspection, testing and assurance results for received components.
Key dependencies / interdependencies **(Include here the cascading impact that may result from the realisation of the hazards)**	▪ Approved suppliers, distributors and original equipment manufacturers. ▪ Limited stock or long lead times may extend the outage and affect dependent operations. ▪ Operational equipment that depends on the component and may be unavailable while the component is replaced.
Controls — Preparedness	▪ Identify high-criticality and long-lead-time components and record maximum tolerable outages. ▪ Establish escalation arrangements where standard approved sources cannot meet operational timeframes. ▪ Maintain verified spares or buffer stock for selected high-criticality components.
Controls — Prevent / minimise likelihood	▪ Purchase critical components from approved and verified suppliers or authorised distributors. ▪ Inspect and test critical components before installation, proportionate to their criticality and the sourcing circumstances. ▪ Monitor supplier performance, non-conformance reports and manufacturer alerts.
Controls — Impact mitigation	▪ Isolate and remove suspected components from service and quarantine related stock. ▪ Engage the manufacturer or specialist provider to verify the component and support restoration.

	▪ Notify relevant internal stakeholders and update procurement controls following confirmed non-conformance.
Owners / status / timeframes	▪ Critical spares and inventory management — Maintenance Manager (In progress; Dec 2026). ▪ Supplier assurance and approved-source controls — Procurement Manager (Implemented; annual review). ▪ Urgent procurement procedure — Operations Manager (Implemented; next exercise Nov 2026).
Residual risk and acceptance	Residual risk assessed as medium due to long lead times for specialist components, reliance on external distributors and the difficulty of identifying sophisticated counterfeits through visual inspection alone. Accepted by the Risk Committee (Jun 2026), subject to completion of the critical-spares review and ongoing supplier assurance.
Review cadence / triggers	▪ component failure, suspected counterfeit or quality-related near miss ▪ an urgent or non-standard procurement ▪ a supplier, distributor or manufacturer alert ▪ a change in supplier, distribution pathway or component specification ▪ repeated non-conformance or warranty issues
Supporting material	▪ Critical component and spare-parts register ▪ Approved supplier and distributor list ▪ Certificates of conformity, inspection results and acceptance testing records ▪ Manufacturer or supplier alerts ▪ Urgent procurement procedure and approval records

Physical security and natural hazard CIRMP entry example

The below example demonstrates how a flooding hazard is captured in an entity's CIRMP.

Field	Example Response
Hazard	Flooding (riverine / flash flooding).
Asset(s) / Site	Primary Operations Centre – **Site A** (includes control room, comms racks).
Scenario	A 1-in-100 year rainfall event causes site access to be cut and water ingress to the ground-floor comms room for 48 – 72 hours.
Why this is material	The scenario could cause disruption to essential monitoring/control capability and communications for an unmanageable period, with potential safety impacts for dependent field operations.
Relevant impact mapping	**Availability:** loss of monitoring/control and communications capability **Reliability:** degraded ability to support dependent field operations.
Evidence supporting likelihood	• Council flood overlays • Historical incidents (2011/2022 events) • Insurer site assessment • Drainage capacity study
Key dependencies / interdependencies (Include here the cascading impact that may result from the realisation of the hazards)	Dependent on the availability of Site A: • Corporate network • Operations of network • Remote access to critical componentry
Controls — Preparedness	• Flood response checklist (roles, contacts, call-out tree) • Lessons learned from 2022 event • Pre-arranged restoration contractor and parts kit on site
Controls — Prevent / minimise likelihood	• Drainage upgrades completed (2025) and quarterly maintenance schedule • Raise thresholds and seal penetrations to comms room • Relocate critical comms equipment above flood line (planned)
Controls — Impact mitigation	• Failover to Secondary Operations Centre – **Site B within 2 hours** • Manual operating procedures for priority functions during failover
Owners / status / timeframes	• Drainage maintenance — Facilities/Ops — Implemented; ongoing quarterly • Sealing thresholds/penetrations — Facilities — Scheduled • Comms relocation — IT/OT Ops — Planned; FY27 milestone • Failover testing — Operations/BCP Lead — Scheduled

Residual risk and acceptance	Residual risk assessed as medium due to remaining exposure to access disruption during extreme events. Risk acceptance approved by the Risk Committee; additional mitigation (equipment relocation) funded for FY26.
Review cadence / triggers	Formal review annually as part of CIRMP review.Trigger review after: • Any flood incident / near miss • Material site changes • Updated flood mapping
Supporting material	• Flood overlay map • Drainage study • Insurance risk report • Maintenance logs • Photos of upgrades • Project plan for relocation • BCP/failover test results • Exercise record and after-action review • Risk acceptance record • Previous CIRMP annual attestations



Australian Government

Department of Home Affairs



CRITICAL
INFRASTRUCTURE SECURITY
CENTRE