Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Guidance for the Critical Infrastructure Risk Management Program

Contents

OVERVIEW

This section provides an overview of the critical infrastructure risk management program obligation

What is the critical infrastructure risk management program obligation?

Specified responsible entities are required to **develop and maintain a Critical Infrastructure Risk Management Program (CIRMP)** for their **critical infrastructure assets (CI assets)**. A CIRMP is a written program that identifies and manages 'material risks' of 'hazards' that could have a 'relevant impact' on a CI asset.

Part 2A of the *Security of Critical Infrastructure Act 2018* (SOCI Act) sets out the requirement to adopt, maintain, comply and review a CIRMP. The *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (the Rules) specify the requirements of a CIRMP and provide further details about hazards to be considered.

An entity's CIRMP must:

- identify each hazard where there is a material risk that the occurrence of that hazard could have a relevant impact on the asset
- as far as it is reasonably practicable to do so, minimise or eliminate any material risk of such a hazard occurring
- as far as it is reasonably practicable to do so, mitigate the relevant impact of such a hazard on the asset
- comply with any other requirements set out in the Rules.

Further information about what a CIRMP should contain can be found in Section 2: Developing the CIRMP.

Separate to the CIRMP, the entity's board, council or other governing body must also submit an **annual report** to the relevant Commonwealth regulator using the approved form.

Further information about annual reports can be found in Section 4: Reporting.

Why is developing a CIRMP important?

Disruptions to critical infrastructure can have serious implications for business, governments and the community, affecting security of resources, supply and service continuity, and damaging economic growth. Putting in place a robust risk management program will help you to:

- Continue to provide your essential services that our communities and economy rely upon.
- Recover more quickly from incidents that impact your CI asset.
- Protect your business' reputation and financial viability.

CIRMPs are intended to uplift core security practices that relate to the management of CI assets. They ensure responsible entities take a holistic and proactive approach toward identifying, preventing and mitigating material risks from all hazards.

Responsible entities are best placed to develop a risk process that suits their assets, noting many organisations have existing risk management practices in place. The Cyber and Infrastructure Security Centre (CISC) wants the CIRMP obligation to complement and where relevant, enhance existing practices.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

SECTION 1: General guidance

This section outlines which CI assets are covered by the CIRMP obligation and what responsible entities need to do by when

Which classes of CI assets are subject to the CIRMP obligations?

CIRMP obligations apply to the responsible entities for CI assets in the following asset classes, which are defined in the SOCI Act:

Sector	Asset Class	CIRMP
Communications	Broadcasting	Yes
	Domain Name Systems	Yes
	Telecommunications	No
Data Storage or Processing	Data Storage or Processing	Yes
Defence Industry	Defence Industry	No
Energy	Electricity	Yes
	Energy Market Operator	Yes
	Gas	Yes
	Liquid Fuels	Yes
Financial Services and Markets	Banking	No
	Financial market Infrastructure (Payment Systems only)	Yes
	Insurance	No
	Superannuation	No
Food and Grocery	Food and Grocery	Yes
Health Care and Medical	Hospitals	Yes
Higher Education and Research	Education	No
Space Technology	No defined Asset Class	No
Transportation	Aviation	No
	Freight Infrastructure	Yes
	Freight Services	Yes
	Public Transport	No
	Ports	No
Water and Sewerage	Water	Yes

Responsible entities for assets that hold a strategic level hosting certificate issued by the Digital Transformation Agency do not need to comply with the CIRMP obligations. However, they must comply with Part 2AA of the SOCI Act. This provision requires responsible entities to provide an annual report in the approved form to the Centre detailing if a hazard had a significant relevant impact on one or more of those assets and the effectiveness of any action taken by the entity to mitigate the impact. The reporting period is the Australian financial year and the report must be submitted within 90 days of the end of the financial year.

This obligation impacts a small number of entities as listed on the Digital Transformation Agency's website.

When do I need to act?

The Rules commenced on 17 February 2023, meaning you need to act if you are a responsible entity for a CI asset in one of these asset classes.

You have until the end of a 6-month grace period to adopt a CIRMP. In practice, this means you will have documented the material risks and controls in place to minimise material risks to your CI asset, and the mitigations that will be put in place over time. Entities must then take reasonable steps to comply with the CIRMP, through implementing controls and mitigations. The CISC does not expect all mitigations to be in place within the 6-month grace period. The Centre suggests better practice is for an entity's board to ratify the CIRMP once developed.

Additionally, entities have a further 12 months to meet the CIRMP cyber security framework requirements. This is in recognition of the time it can take to select and implement a framework at an enterprise level. Further details on the cyber security framework requirements are outlined in Section 3: CIRMP rules in practice, Cyber & Information Security Hazards.

Once implemented, entities need to review the CIRMP on a regular basis, keep it up to date, and comply with annual reporting requirements – see Section 5: CIRMP maintenance.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

My asset(s) are covered by the obligation. What do I need to do?

1 Develop CIRMP & Comply with Rules

- Identify hazards applicable and material risks to your CI asset (section 7 of the Rules).
- For each material risk, be sure to consider the impact on your assets if the risk was to eventuate.
- Implement mitigations or eliminate material risks as far as is reasonably practicable (section 30AH of the SOCI Act and section 7 of the Rules).
- Understand requirements of the Rules and identify activities required to comply with the Rules to mitigate material risks from all hazards as well as specified hazards prescribed in the Rules (sections 8-11 of the Rules).
- Refer to Section 2: Developing the CIRMP and Section 3: CIRMP rules in practice

There is no prescribed format for a CIRMP, and nor is the CIRMP intended to supplant existing risk management processes. Rather, responsible entities are encouraged to incorporate existing risk management frameworks and processes into the CIRMP.

2 Annual report to CISC

- Submit an Annual Report approved by entity's board, council or other governing body, in the approved form, to the relevant Regulator within 90 days of the end of the relevant Australian financial year.
- The Centre may review a sample of CIRMPs following the grace period.
- Refer to Section 4: Reporting

3 Continuous Obligations

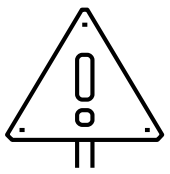
- Maintain the CIRMP (section 30AC of the Act)
- Review the CIRMP on a regular basis (section 30AE and section 7 of the Rules) and
- Update the CIRMP, by taking reasonable steps to ensure that there is a process or system in the CIRMP to keep the program up to date (section 30AF and section 7 of the Rules)
- Refer to Section 5: CIRMP maintenance

SECTION 2: Developing the CIRMP

This section provides additional detail on developing the CIRMP and what must be included in a CIRMP, as outlined in the Rules

What are the requirements for a CIRMP?

Identify each 'hazard' where there is a 'material risk' that the occurrence of the hazard could have a 'relevant impact' on the asset



What is a hazard?
Section 3 of the Rules define the four key hazard vectors.

- **Cyber** and **information security** hazards
- **Personnel** hazards
- **Physical security** and **natural** hazards
- **Supply chain** hazards

Refer to Section 3: CIRMP rules in practice for further guidance on hazard vectors

What is a material risk?
Section 6 of the Rules defines material risk. This includes a risk that could result in the occurrence of the following:

- a **stoppage or major slowdown** of the asset's function for an **unmanageable period**
- a **substantive loss of access to**, or deliberate or accidental manipulation of, **a critical component** of the asset
- an **interference** with an asset's operational technology or information communication technology **essential to the functioning of the asset**
- 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
- **remote access to operational control** or operational monitoring systems of the asset

What is a relevant impact?
The Rules refer to relevant impact as defined in section 8G of the SOCI Act. This describes when a hazard directly or indirectly impacts the:

- **availability** of the asset
- **integrity** of the asset
- **reliability** of the asset or
- **confidentiality** of computer data, stored information, or information about the asset.

Even if some hazards are more relevant than others, it is important that your CIRMP **considers all hazards** independently, as well as where hazards converge to result in material risks. This may require you to collaborate with internal and external stakeholders to ensure hazard vectors are considered concurrently and mitigations are sufficiently comprehensive.

What are the requirements for a CIRMP? (Cont.)

References to relevant legislation within this section

CIRMP Rules
SOCI Act

Outline the process or system in place

Subsection 7(1) of the Rules require that responsible entities **must** establish a process or system to:

- Identify the operational context of the asset
    - The CIRMP must describe the outcome of the process or system mentioned as part of this operational context. That is, to provide the detail of what that process or system does.
- Identify the material risks to the asset
- **As far as it is reasonably practicable**, minimise or eliminate the material risks
- **As far as is reasonably practicable**, mitigate the relevant impact of each hazard
- Review the CIRMP
- Keep the CIRMP current

"**As far as is reasonably practicable**" allows entities to determine how they address material risks and relevant impacts in relating to the operating context of their business. Mitigations are expected to be commensurate with factors such as business size, maturity and income.

Minimise risks to prevent incidents

Subsection 7(1)(c) of the Rules require that a responsible entity **must** establish and maintain a process or system in the CIRMP to minimise or eliminate the material risk of hazards occurring, *as far as is reasonably practicable*. Entities should consider both proactive risk management as well as establishing and managing processes to detect and respond to threats as they are being realised to prevent the risk from eventuating.

Mitigate the impact of realised incidents

Subsection 7(1)(c) of the Rules require that a responsible entity **must** establish and maintain a process or system in the CIRMP to mitigate, *so far as is reasonably practicable*, the impacts of a hazard, to promote recovery from the impact as quickly as possible. Mitigation activities must be based on documented processes or systems that can be activated as required.

Describe interdependencies between the entity's asset and other CI assets

An entity's CIRMP must describe how their CI assets interact or intersect with CI assets owned or operated by other responsible entities. This includes assets within the same sector and other sectors, as well as up and downstream of the entity's asset(s). This ensures that entities consider the operational extent of networks of assets so that mitigations are appropriately broad.

Identify each person in the entity who is responsible for:

- Developing and implementing the CIRMP
- Reviewing and keeping the CIRMP up to date

An entity's CIRMP must also include the contact details for the named person(s) above.

Outline the risk management methodology

Entities are required to develop and describe a methodology or principles used to identify and implement appropriate controls to:

- Minimise or eliminate the material risks of the hazard, as far as is reasonably practicable; and
- Mitigate the relevant impact of the hazard were it to occur.

This must be done for each individual risk identified.

Risk management methodologies should:

- Be consistent with the overall goals and culture of the entity
- Clearly identify the roles and responsibilities for staff involved in developing and implanting controls
- Consistently review the appropriateness of controls given the evolving nature of risk

Identify your critical components

Risks to critical components should be considered and mitigated as appropriate.

A critical component of a CI asset is part of the asset that, if that part was absent, damaged or compromised, the entity assesses:

- would prevent the proper function of the asset; or
- could cause significant damage to the asset.

What are the requirements for a CIRMP? (Cont.)

References to relevant legislation within this section — CIRMP Rules, SOCI Act

Describe the circumstances in which an entity will review its CIRMP

The Act requires that a responsible entity must review its CIRMP on a regular basis. Subsection 7(2)(f) of the Rules requires that the entity describe the circumstances in which it will review the CIRMP.

A responsible entity must consider situations in which it is appropriate to review and potentially update their CIRMP. Catalysts for review may be determined by the entity's existing structures and protocols.

Triggers for review may include changes in the operating environment, including emerging threats; occurrence of a hazard that resulted in a material risk eventuating; a routine review schedule; the introduction of industry standards changes to an existing CI asset; or acquiring a new CI asset.

At a minimum, a CIRMP should be reviewed **once every 12 months** to ensure it is current.

Further requirements regarding review of a responsible entities CIRMPs are detailed in Section 5: CIRMP maintenance.

Comply with hazard-specific requirements

For the purposes of section 30AH(1)(c) of the SOCI Act, sections 8-11 of the Rules detail specific requirements for each of the four hazard vectors: cyber and information security, personnel, supply chain, and physical security and natural hazards. Entities must have processes in place to minimise or eliminate material risks, and to mitigate the relevant impact of these hazards on CI assets.

The risk-specific requirements for a responsible entity's CIRMP are described in Section 3: CIRMP rules in practice.

Entities should note that the Rules may be updated by the Minister for Home Affairs from time-to-time. Should this occur, consultation is required before any amendments are finalised and applied.

As such, an entity's CIRMP should be capable of incorporating additional future requirements.

The Centre has published sector-specific guidance on assessing risks to Australia's critical infrastructure to assist stakeholders adapt existing risk practices and help organisations understand their CI risks. This guidance is available on the CISC Resources website.

SECTION 3: CIRMP rules in practice

This section will assist responsible entities to identify and treat risks to their CI assets arising from an "all hazards" approach

Application of the Rules by Hazard

Australia's critical infrastructure may be subject to threats from multiple vectors, either independently or concurrently.
The following information provides details on considerations and risk-specific requirements to help your organisation assess material risks and implement your CIRMP.

Cyber & Information Security Hazards

What the Rules say

Section 8 of the Rules provide specific requirements for this hazard vector, they are that an entity must:

- Establish and maintain a **process or system** in the 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** the relevant impact of a cyber and information security hazard on the CI asset.
- Within 12 months of the expiry of the 'grace period'
- Comply with one of the frameworks specified in subsection 8(4); or,
- comply with an equivalent framework

Cyber frameworks specified in subsection 8(4) of the Rules are provided on the following page for reference.

What is an equivalent framework?

Entities should consider their risk management methodology and the cyber and information security hazards that are most relevant to their asset when considering implementing cyber security frameworks not listed in the Rules.

If an alternative framework better addresses the risk vectors threatening an entities critical assets then the CISC would consider this a valid equivalent framework.

The CISC is wanting to proactively engage with entities considering implementing alternative frameworks. Please contact enquiries@CISC.gov.au if your organisation is looking to explore alternative cyber security frameworks.

Cyber & Information Security Hazards

How this may apply for a CI asset

An entity's CIRMP **must describe** the cyber and information security hazards that could have a relevant impact on the asset.

Some examples of hazards you **may** consider are:

- **Phishing:** where fraudulent emails are sent to specific companies or individuals.
- **Malware:** malicious software used to deny access, obtain information, gain control or disrupt systems.
- **Credential harvesting:** often facilitated through phishing, it involves using legitimate credentials and built-in tools to gain access to systems, as to be less detectable than malware.
- **Denial-of-service (DoS):** involves flooding systems with traffic to overload and disable them.

To **minimise or eliminate** a material risk, and **mitigate** a relevant impact for **cyber and information security hazards**, responsible entities may consider:

- **Anti-phishing techniques** such as employee education policies and installing anti-phishing software.
- Developing an **incident response plan** detailing the actions to take in response to a cyber security incident.
- **Regularly testing the effectiveness of controls**, including vulnerability testing of critical applications.
- Using **penetration 'pen' tests,** or simulated cyber attacks against their firewalls and all components of their IT and OT infrastructure to assess vulnerabilities.
- **Ensuring there is sufficient segmentation** of systems to prevent dual compromise.
- **Ensuring access privileges** to critical systems such as the Active Directory and IT wikis are **checked and updated regularly.**

NOTE: The Cyber & Information Security Hazards rules are separate to any Enhanced Cyber Security Obligations that may apply to assets that are declared Systems of National Significance

Cyber frameworks

Subsection 8(4) specifies the document and condition (where indicated) with which a responsible entity must comply (unless complying with an alternative equivalent framework)

Document	Condition
Australian Standard AS ISO.IEC 27001:2015	
Essential Eight Maturity Model published by the Australian Signals Directorate	Meet maturity level one as indicated in the document
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	Meet maturity level one as indicated in the document
The 2020-21 AESCSF Framework Core published by Australian Energy Market Operator Limited (ACN 072 010 327)	Meet security profile one as indicated in the document

Personnel Hazards

What the Rules say

Subsection 9(1) of the Rules provides specific requirements for this hazard vector:

- **identify** the entity's **critical workers**
- permit a critical worker access **to critical components** of the asset only where the worker has been **assessed to be suitable** to have such access
- as far as it is reasonably practicable to do so – **minimise or eliminate material risks** arising from:
    - malicious or negligent employees or contractors
    - The off-boarding process for outgoing employees and contractors

Identifying critical workers

A critical worker is an employee, intern, contractor or subcontractor of an entity:

- the entity assesses that their absence or compromise would prevent the proper function of the CI asset or could cause significant damage to the asset; AND
- who has access to, or control and management of, a critical component of the CI asset.

To identify critical workers, consider:

1. **What are the essential components** or systems of your assets?

2. **Who has responsibility** over, access to, control over or management of these assets? Including critical control points within IT systems.

In practice critical workers could include roles such as Chief Information Security Officer, control room operators, or workers such as IT administrators with unrestricted administrator rights and access to systems. Entities are best placed to understand the criticality of their operations and employees.

Note: the process for identifying critical workers has the same practical application as identifying critical positions. The only difference is that entities must name the employee holding the critical position. Entities will need to be active in updating their CIRMP to reflect the movement of these people within or out of the organisation.

How this may apply to a CI asset

When considering how to **minimise or eliminate** a material risk, and **mitigate** a relevant impact for **personnel hazards**, prioritise:

- **Controlling** who is allowed access to your critical asset. This includes 'access controls – both physical and digital - to authorised individuals only. Further, controls should include restricting connection of removable media and unapproved devices to your network.
- **Background checking** of critical workers – whilst not mandatory, the **AusCheck** service is available to responsible entities (see further below). Entities can use alternate suitable background checking services if preferred.
- **Heightened monitoring of personnel** with access to critical systems, to detect malicious insiders (employees or contractors who use their position and access to steal data or negatively interact with assets and operations).
- **Cyber security training** for staff, including around data storage, anti-phishing and password security.

Home Affairs offers a background checking service for security-sensitive critical infrastructure sectors in Australia called AusCheck. These background checks are an important way to mitigate trusted-insider personnel risks working in sensitive CI sectors.
To manage personnel hazards, you may carry out background check under the AusCheck scheme at regular intervals however use of AusCheck is optional, and you may use other schemes or processes. It is up to individual entities to decide how best to assess the personnel risks workers pose, and how to manage these risks.
For more information on AusCheck please visit the AusCheck background checking page on our website for more information.

Further guidance on the personnel security vector, including AusCheck will become available in coming months.

Supply Chain Hazards

What the Rules say

Section 10 of the Rules provides that an entity **must establish** and **maintain** in the CIRMP a process or system to minimise or eliminate the following material risks:

- **unauthorised access**, **interference** or **exploitation** of the asset's supply chain; and
- **misuse of privileged access** to the asset by any provider in the supply chain; and
- **disruption** of the asset due to an issue in the supply chain; and
- **arising from threats** to people, assets, equipment, products, services, distribution and intellectual property within supply chains; and
- **arising from major suppliers**; and
- any **failure or lowered capacity** of other assets and entities in the entity's supply chain.

Additionally, entities must mitigate the relevant impact of supply chain hazards including the above, on the CI asset.

Subsection 10(2) of the Rules provides that entities must consider whether the CIRMP lists the entity's major suppliers when adopting, reviewing and varying the CIRMP. Section 3 of the Rules defines **major suppliers** as '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.'

The CIRMP obligations recognise that robust visibility and oversight are key to managing potential supply chain disruptions and security risks from exposure to major suppliers. This must be done on an ongoing basis. When compiling the list of major suppliers for the CIRMP, entities should ask themselves whether reasonable steps have been taken to ensure that the list is:

- **Complete:** reasonable steps have been taken to list all major suppliers, with no gaps.
- **Accurate:** the details of the major suppliers are free of major errors and accurately identify the suppliers.

How this may apply to a CI asset

To **minimise or eliminate** a material risk, and **mitigate** a relevant impact for **supply chain hazards**, responsible entities **may** consider:

- Ensuring major suppliers with access to sensitive data have sufficient security personnel and cyber security resilience policies built into contract arrangements
- Identifying and reducing dependencies and supply chain bottle necks through diversification of vendors

What constitutes your 'supply chain'?

There is no prescriptive definition of a 'supply chain' in the Rules. The extent of your entity's supply chain is contextual. You should consider the essential goods and services required to operate your critical asset and deliver goods and services. To do this, consider:

1. **What are the processes necessary** to produce and deliver your essential goods and / or services?
2. **Who are the vendors** that supply the services and products your critical asset relies upon to operate? E.g. raw materials, packaging, transportation and management software.
3. **What essential processes and third parties** do your vendors rely upon to provide you with goods and services?
4. **What countries** do your vendors operate from?
5. **Who owns and operates** your vendors?

What is a major supplier?

To determine who is a major supplier, entities should ask themselves whether any vendor's products or services enable a significant influence over the security of the entity's CI asset. For example, the supplier may be subject to adverse direction from foreign actors, the vendor's poor cyber security posture may expose them to adverse external interference, or the vendor may in some other way transfer unreasonable risk to an entity's system.

To determine material supply chain risks, including major suppliers, responsible entities should consider:

1. **If a supplier were unable to ensure continuous supply of goods or services**, what would happen? Would your asset stop functioning or are there alternative suppliers that could guarantee the required goods and services?
2. **How strong is the market supply** of these goods and services?
3. **Who has potential adverse influence** and control over your suppliers?

Physical Security & Natural Hazards

What the Rules say

Subsection 11(1) of the Rules provides that you **must** establish and maintain a process or system to:

- Identify the **physical critical components** of the CI asset
- 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
- respond to incidents where **unauthorised access** to a physical critical component occurs
- **control access** to physical critical components, including restricting access to only those individuals who are **critical workers** or accompanied visitors
- 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.

Section 3 and subsection 11(2) of the Rules require that in a CIRMP you **should** consider and describe:

- **Physical security hazards**: the unauthorised access to, inference with, or control of CI assets, to compromise the proper function of the asset or cause significant damage to the asset.
- **Natural hazards**: including fire, flood, cyclone, storm, heatwave, earthquake, tsunami, space weather or biological health hazard (such as a pandemic).

How this may apply to a CI asset

When considering how to **minimise or eliminate** a material risk, and **mitigate** a relevant impact for **physical security and natural hazards**, prioritise:

- **Locking down** industrial control systems, including HVAC, cameras, fire alarm panels from attacks through access privileges and onsite security.
- Ensuring **critical components** are constantly patrolled or monitored by security staff.
- Fostering **infrastructure resilience** and preparedness through contingency planning, emergency exercises and simulations.
- **Implementing physical** access controls, such as perimeter fencing, biometric access-keys or time-locked access for an assets critical component.
- Developing and maintaining a **bush fire survival plan** which could include controlled burning of surrounding forestry or the installation of bush fire sprinklers.
- **De-clustering** of key assets i.e. spreading infrastructure across multiple sites and maintaining backup infrastructure to increase resilience.
- Installing **CCTV** or **motion detection sensors** to improve the ability of security staff to detect unauthorised access.

Further information on **critical workers** provided under Personnel Hazards (within this section)

Further information on **critical components** can be found in Section 2: Developing the CIRMP

SECTION 4: Reporting

This section provides guidance on the annual reporting requirements applicable to CIRMPs

What does the Annual Report need to contain?

Section 30AG of the SOCI Act requires the report to be in the approved form, which includes the following:

- A declaration that the CIRMP was or was not up to date at the end of the Australian financial year
- *IF* a hazard occurred that had a significant relevant impact on a CI asset(s) during the financial year, the report must cover:
  - what that hazard was (or continues to be)
  - whether the CIRMP was effective in mitigating the significant relevant impact of the hazard on the CI asset(s)
  - whether any variations to the CIRMP were made during the year as a result of the hazard occurring, and what these changes were
- In the case where the responsible entity has a board, council or other governing body – the annual report must be approved by the relevant body

The annual report does not need to contain the CIRMP. However, it must assure the CISC or other relevant regulator whether the program remains up-to-date and appropriate (for more information on who is the relevant regulator see 'who receives the Annual Report?' below).

What will the information in the Annual Report be used for?

Annual reports will be used by CISC to better understand the threat environment in each sector. This enables the CISC to provide meaningful assistance to industry when subject to a hazard and advise entities on ways to further enhance the security and resilience of CI assets.

Who receives the Annual Report?

Entities must submit the Annual Report to the relevant Commonwealth regulator. The CISC is the relevant regulator for all assets, except for payment systems whose responsible entities must submit their annual report to the Reserve Bank of Australia.

When is the report due?

The report must be submitted within 90 days after the end of each Australian financial year the entity had a CIRMP in place.

Due to the CIRMP grace period, responsible entities are not obligated to provide an annual report for the 2022-2023 Australian financial year. The first annual report required under the Rules is for the 2023-2024 Australian financial year. As entities have 90 days after the end of the financial year to submit this annual report to the relevant regulator, the first report must be submitted between 30 June 2024 and 28 September 2024,

For the 2022-23 Australian financial year, the CISC strongly encourages entities to submit an annual report voluntarily, as a pulse check on how you are implementing the CIRMP. This report does not need to be overly detailed and should be viewed as an opportunity to provide assurance that entities are taking steps to enhance risk management procedures.

Further guidance on annual reporting requirements and the approved form will be released over coming months.

As a key part of Australia's critical infrastructure, the resilience of your operations are relied on to deliver services to Australians. The CISC and industry are jointly committed to ensuring good risk management practices are in place.

The annual report is an important mechanism for Boards to assess security risk management and also to provide the Centre with visibility of how critical infrastructure entities are managing security risks – both holistically and at an individual asset level. It will allow the Centre to form a view of how risks are being managed, what hazards are impacting critical infrastructure, and will be an important input in the formation of our advice back to industry.

Consistent with our regulatory posture, this is about working proactively with industry for improved outcomes for all. The CISC is not interested in punishing organisations trying to do the right thing.

SECTION 5: CIRMP maintenance

This section provides guidance on how responsible entities remain compliant with the CIRMP obligation

How do I maintain a CIRMP?

In addition to having a CIRMP and submitting an annual report, SOCI Act requires that entities uphold the following requirements.

Comply

Section 30AD of the SOCI Act requires that a responsible entity **must** comply with the CIRMP.

This includes adhering to mitigations and any other requirements that have been included, such as conducting background checks on staff prior to onboarding.

Review

Subsection 7(1)(d) of the Rules requires that a responsible entity **must** maintain a process or system to review the CIRMP. This ensures compliance with section 30AE of the SOCI Act.

Entities are required to review their CIRMP on a regular basis. The purpose of the review is to ensure currency of identified hazards, adequacy of mitigations and appropriateness of risk identification mitigation.

Additionally, subsection 7(2)(f) of the Rules require a responsible entity describe the circumstances in which the entity will review the CIRMP. Details on this requirement are included in Section 2: Developing the CIRMP.

At a minimum, a CIRMP should be reviewed **once every 12 months** to ensure it is current.

Update

Subsection 7(1)(e) of the Rules requires that a responsible entity **must** keep the CIRMP current. This ensures compliance with section 30AF of the SOCI Act.

Section 30AF also requires entities to take all reasonable steps to ensure the program is up to date. Subsection 7(2) of the Rules sets out matters that entities must consider when reviewing a CIRMP or deciding whether to vary the CIRMP.

When reviewing and updating a CIRMP, entities must have regard for the same matters in the Rules as when the CIRMP was first drafted. Any variation must be made with consideration of these matters.

SECTION 6: Further information

Trusted Information Sharing Network

Entities are strongly encouraged to join the Trusted Information Sharing Network (TISN).

TISN is industry and all levels of government's primary way of engaging to enhance the security and resilience of critical infrastructure.

The TISN provides a secure platform for CI entities to discuss threats and other issues within an industry context.
Find out more about how to join the TISN on our website or contact us at CIR@homeaffairs.gov.au.

Where can I find more information?

More information on the protection of Australia's critical infrastructure can be found on the Centre's website.

The key **legislative instruments** are listed below and can be found here:

- Security of Critical Infrastructure Act 2018
- Security of Critical Infrastructure (Critical infrastructure risk management program) Rules
- Security of Critical Infrastructure (Application) Rules
- Security of Critical Infrastructure (Definitions) Rules

A summary of useful information and guidance about SOCI obligations, including on CIRMPs, can be found on the factsheet page of the Centre's website.

Where to from here?

Date	Requirement
17 February 2023	Rules commence
17 August 2023 (6 months after commencement of Rules)	End of 6 month grace period.
18 August 2023	First day of compliance with the CIRMP
17 August 2024 (18 months after commencement of Rules)	Last day for a CIRMP to adopt and comply with the cyber and information security hazards framework
28 September annually	Last day to submit an annual report for the preceding Australian financial year (i.e. ending 1 July to 30 June)
Ongoing	Comply with, regularly review and if required update the CIRMP

If a responsible entity's asset becomes a CI asset after the Rules commence, the responsible entity must meet CIRMP requirements within 6 months of the day the asset became a CI asset, and must meet the cyber and information security hazards framework within 18 months of that day.

Please contact us if you are having problems adopting elements of the CIRMP requirements. This is the start of our journey toward an uplifted CI security posture, and our intent is to work closely with industry to ensure industry understand their obligations.