Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Town Hall – Critical Infrastructure Risk Management Program (CIRMP) obligations and compliance

30 July 2024

OFFICIAL

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Agenda Overview

1. CIRMP Obligations

2. 2024-2025 Regulatory Posture

3. Compliance activities including annual reports

CIRMP Obligations

Date	Requirement
17 February 2023	Rules commenced
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 2024 (90 days after EOFY 2024)	The first annual report for the Australian Financial Year 2023-2024 due for submission
28 September 2025 onwards	Last day to submit an annual report for the preceding Australia Financial Year

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

2024-2025 Regulatory Posture

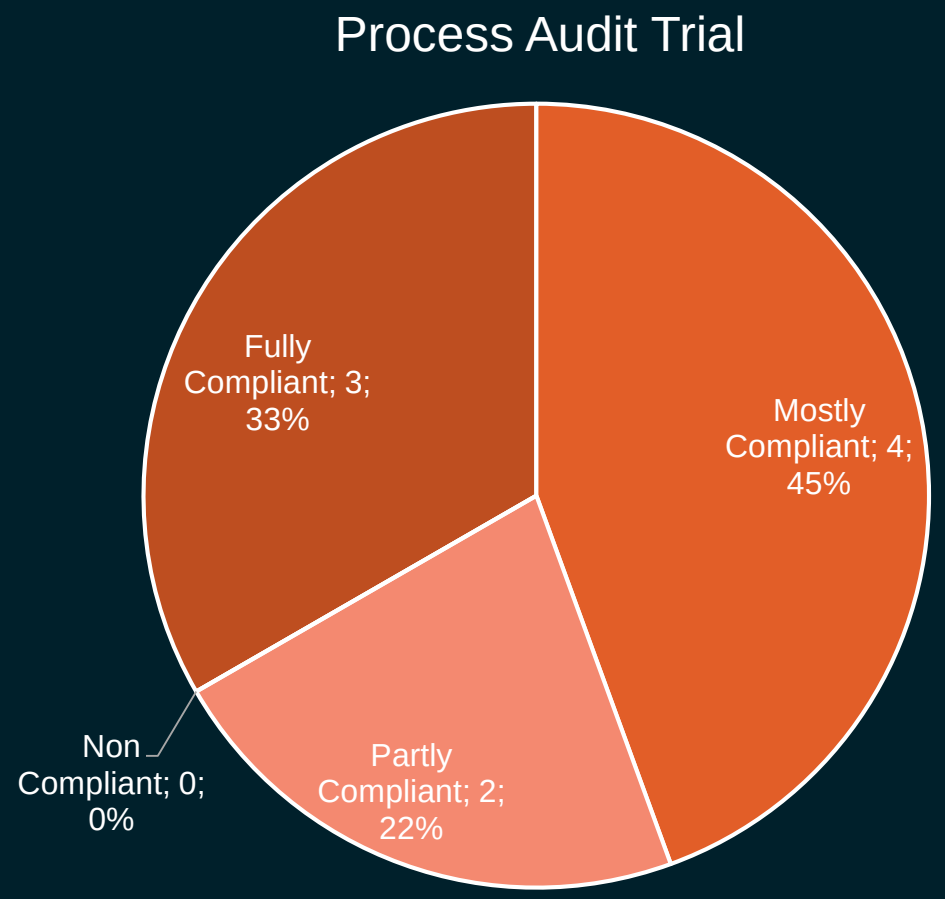
- 2023-24: Compliance focus was on education and awareness raising.
- 2024-25: Compliance Regulatory posture will aim to balance education and awareness raising activities, with compliance activities, in order drive uplift in regulated entity compliance.
- Effective compliance activities support SOCI Act 2018 objective to provide a framework for managing risks relating to critical infrastructure.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

SOCI Act 2018 – Audit Trials

- Limited series of trial audits conducted in Q3 and Q4 2023/24 to test audit process and level of industry compliance with SOCI Act obligations.
  - Ten auditees randomly selected from ten different sectors; nine audits concluded and one to be finalised.
  - Audit reports issued to each entity with findings and where appropriate - with suggested corrective actions for identified non compliances.
- A formal audit program to evaluate compliance with SOCI obligations will commence 2024-2025.



Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

SOCI Act 2018 – Audit Trials – CIRMP Adequacy

- CISC currently undertaking further series of 10 content audits trials.
- Aimed at assessing auditee's CIRMP's adequacy and suitability at identifying and addressing risks to the relevant SOCI Critical Infrastructure Asset(s).
- Key lessons learned from the trials will be shared with stakeholders in August/September 2024.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Trusted Information Sharing Network Survey

- In May-June 2024 a voluntary TISN survey was conducted regarding expected compliance with upcoming CIRMP deadline of 17 August 2024 for the cyber and information security framework.
- Results from the 21 responses received:

Compliance level	Response
Fully compliant	11
Mostly compliant	1
Somewhat compliant	8
Not compliant	1

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Compliance Activities

- CISC does not have the ability to grant time extensions for entities to meet CISC obligations. Engage proactively and contact the CISC via enquiries@CISC.gov.au.
- For non-compliance with the CIRMP cyber security framework requirement, the entity should provide the following information:
  - Components of cyber security framework in place.
  - Outstanding components of cyber security framework.
  - Any roadblocks that are preventing full compliance.
  - A Board approved plan and timeframe for coming into compliance with periodic progress reporting for achieving compliance.
- CISC will review the reasons and circumstances for non-compliance, as part of our compliance and enforcement activities. We will also monitor periodic progress reporting to ensure entities become compliant as soon as possible.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Updates to the CIRMP web form

- It is a requirement to use the approved web form on the CISC website.
- Web form has been redesigned to provided additional guidance and prompt for specific information sought by CISC.
- The CIRMP Annual Report web form provides capability to attach information to support your Annual Report such as:
  - Audits or reports commissioned to provide assurance to your board that your entity is in compliance with its CIRMP obligation.
  - Any relevant supporting information.
  - Any relevant reports on hazard and risk mitigation.

Responsible Entity Risk Management Program - Annual Report

Part 2A of the *Security of Critical Infrastructure Act 2018* (SOCI Act) requires Responsible Entities for critical infrastructure assets to have and comply with a Risk Management Program (RMP). Responsible Entities must submit an Annual Report relating to its RMP to the relevant Regulator within 90 days of the end of the relevant Australian financial year. The Annual Report must be approved by the Entity's board, council or other governing body, and must be submitted using this form.

This form must be completed within 90 days after the end of each financial year. It is recommended that you make a copy of this form for your records.

Section 4: Further Information and Attachments

Attach any relevant documentation. Suggested list of attachments to support your application include:

- Any audits or reports you may have commissioned to provide assurance to your board, council or governing body that the Responsible Entity is in compliance with its RMP obligation.
- Any relevant supporting information regarding your Responsible Entity's approach and processes to manage risks to its critical infrastructure assets.
- Any relevant reports on hazard and risk mitigation.

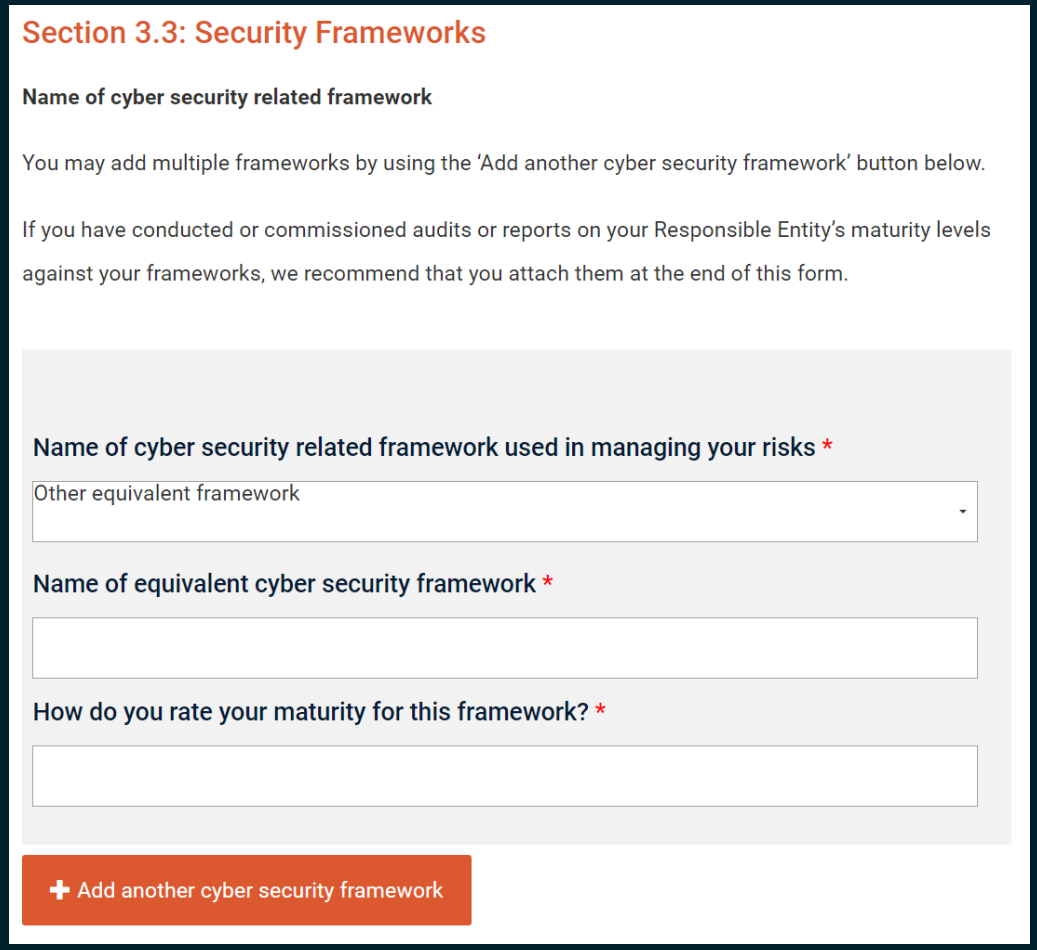
There is no requirement to submit your RMP with this Annual Report. CISC does not provide advice on RMPs.

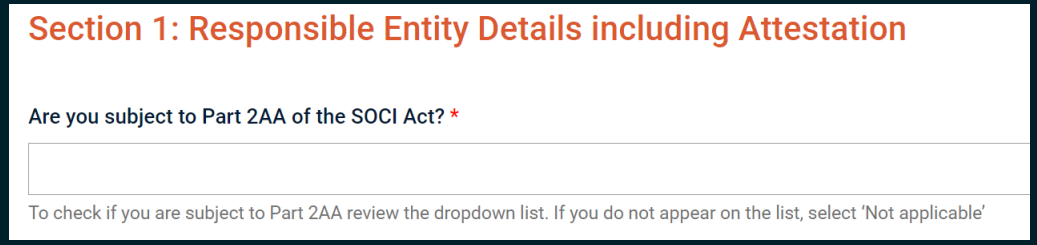
Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Updates to the CIRMP web form

- The web form is intended to be used by both Part 2A and Part 2AA entities. As such, not all fields will be relevant for all entities.
- Part 2AA entities are a small number of responsible entities that hold a strategic level hosting certificate issued by the Department of Home Affairs.
- Section 3.3 Security Frameworks is now shown by default unless Part 2AA is selected as applicable (no obligation for RMP).





Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Cyber Security Framework

- Obligation to adopt a specified framework and level of maturity (or equivalent) ONLY turned on from 17 August 2024.
- Information about framework used and maturity against framework sought as part of 2023-24 annual report. This is intended to help inform our understanding of industry maturity but will not be used for compliance purposes.
- CIRMP Rules specify five frameworks for cyber and information security hazards or equivalent. If using an alternative framework – outline why it is equivalent.

Item	Document	Condition
1	Australian Standard *AS ISO/IEC 27001:2015*	
2	*Essential Eight Maturity Model* published by the Australian Signals Directorate	Meet maturity level one as indicated in the document
3	*Framework for Improving Critical Infrastructure Cybersecurity* published by the National Institute of Standards and Technology of the United States of America	
4	*Cybersecurity Capability Maturity Model* published by the Department of Energy of the United States of America	Meet Maturity Indicator Level 1 as indicated in the document
5	*The 2020-21 AESCSF Framework Core* published by Australian Energy Market Operator Limited (ACN 072 010 327)	Meet Security Profile 1 as indicated in the document

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Security Framework

- As part of 2023-24 CIRMP Annual Report process we are seeking to gather information on what security frameworks are used by industry to address the non-cyber security hazards.
- No standard or maturity ratings are currently specified for the CIRMP to manage non-cyber security hazards.
- CIRMPs are required to cover all hazards comprising:
  - Physical security
  - Natural hazards
  - Personnel hazards
  - Supply chain hazards
  - Cyber security hazards
  - Information security hazards

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Questions?

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Thank you for attending

Website: www.cisc.gov.au

Email: enquiries@cisc.gov.au

Phone: 1300 272 524

Follow the CISC socials on X, LinkedIn and Instagram

OFFICIAL