Regulatory obligations

All critical infrastructure asset owners, operators, and direct interest holders must meet their legal obligations under the *Security of Critical Infrastructure Act 2018* (the SOCI Act) *(https://www.legislation.gov.au/Series/C2018A00029)*. The obligations that apply to your business will depend on the kind of critical infrastructure asset that you own, operate, or have a direct interest in.

These obligations seek to make risk management, preparedness, prevention and resilience business as usual for the owners and operators of critical infrastructure assets. They will also improve information exchange between industry and government to build a more comprehensive understanding of the national threat environment.

The obligations that you must meet will depend on whether you are a responsible entity or a direct interest holder for an asset.

Responsible entities own or operate the asset. Each asset class includes their own specific definition for a responsible entity in their sector. The responsible entity for each asset class is defined in section 12L of the SOCI Act. They must provide operational information in relation to the asset.

A direct interest holder is an entity (e.g. individual, company or trust) that holds either:

- a direct or joint interest of at least 10% in the asset, together with any associates
- an interest in the asset that puts the entity in a position to directly or indirectly influence or control the asset.

For more information about what a critical infrastructure asset is, go to our page on the *Security of Critical Infrastructure Act 2018* (SOCI) *(/legislation-regulation-and-compliance/soci-act-2018)*.

If you are not sure whether these obligations apply to your critical infrastructure asset, read our Critical Infrastructure Asset Class Definition Guidance (2MB PDF) *(/resources-subsite/Documents/cisc-factsheet-asset-class-definition-guidance.pdf)*.

Obligation to notify data service providers

Entities must notify external data service providers if they are storing or processing business critical data for a critical infrastructure asset. This ensures that companies that handle sensitive data are aware that they may also have obligations under the SOCI Act. It will also ensure that they treat the security of the data appropriately.

This obligation applies to all critical infrastructure assets.

For more information on how this obligation might apply to you, read the Obligation to notify data storage or processing providers Factsheet (156KB PDF) *(/resources-subsite/Documents/cisc-factsheet-subsection-12f-obligation-to-notify-guidance.pdf)*.

Positive security obligations

There are three primary security obligations which apply to most critical infrastructure assets.

Provide operational and ownership information to the Register of Critical Infrastructure Assets

The Register of Critical Infrastructure Assets (the Register) requires reporting entities to provide ownership, operational, interest and control information to government. Reporting entities are either direct interest holders or the responsible entity of critical infrastructure assets.

Responsible entities, or an agent of the responsible entity, must provide operational information about the asset.

Direct interest holders must provide interest and control information about the asset.

An entity may be both the responsible entity and a direct interest holder in relation to the asset. In this case, they would be responsible for reporting both operational information, and interest and control information to the Register.

The Register helps the government understand the ownership and operational arrangements of critical infrastructure assets. This includes how different assets may interact with or rely on each other.

This information is used by the government to help industry reduce and manage risks to critical infrastructure assets. The government does this by providing timely advice, guidance and information on emerging risks. This will help you to continue providing your essential services that our communities and economy rely upon.

The Register is not public, and all information contained on it is protected information under the SOCI Act *(/how-we-support-industry/regulatory-obligations/protected-information)*. This means the information cannot be used or disclosed except in limited circumstances. There are consequences to disclosing protected information outside of these circumstances. Any personal or sensitive information reported to the Register will also be subject to the *Privacy Act 1988* *(https://www.legislation.gov.au/Series/C2004A03712)*.

If you fail to register or update information on the Register, you may be penalised.

For more information and examples of how this obligation may affect you, see our Register of Critical Infrastructure Assets Guidance Factsheet (413KB PDF) *(/resources-subsite/Documents/register-critical-infrastructure-assets.pdf)*.

What operational information is required?

Responsible entities must provide operational information. You are encouraged to provide as much information and context as possible. This will inform the government's understanding of the operation of, and risks associated with, critical infrastructure assets.

If you are registering your asset for the first time, you must complete the Registration form for the Responsible Entity of a Critical Infrastructure Asset *(/resources/online-forms/notification-of-existing-registration-of-critical-infrastructure-assets)*.

You are required to provide information about:

- the location of the asset
- the area the asset services
- the arrangements under which another entity operates the asset or a part of the asset
- the arrangements under which relevant data types are managed by a third-party.

Once you have provided this information, you will need to make sure it remains up to date.

Examples of events that may require updating include changes to:

- contact information
- the reporting entity
- operator or data arrangements.

If you need to update an existing registration, complete the Responsible Entity: Notification of change to an existing registration on the Register of Critical Infrastructure Assets form *(/resources/online-forms/notification-of-existing-registration-of-critical-infrastructure-assets)*.

What interest and control information is required?

Direct interest holders must provide interest and control information. You are encouraged to provide as much information and context as possible. This will inform the government's understanding of the ownership and control of, and risks associated with, critical infrastructure assets.

You must provide the interest and control information within 6 months of the day the asset became a critical infrastructure asset. You can do this by filling out the Direct Interest Holder of a Critical Infrastructure Asset registration form *(/resources/online-forms/interest-holder-of-critical-infrastructure-asset)*. The information that you need to provide is listed in section 6 of the SOCI Act *(https://www.legislation.gov.au/Series/C2018A00029)*.

You must provide us with information about:

- the type and level of the interest the direct interest holder holds in the asset
- the influence or control the first entity is able to directly or indirectly exercise in relation to the asset

- the ability of a person, who has been appointed by the direct interest holder to the body that governs the asset, to directly access networks or systems that are necessary for the operation or control of the asset
- each other entity that is able to directly or indirectly influence or control relevant entities.

You must update us of any changes to this information within 30 days by filling out the Direct Interest Holder: Notification of change to an existing registration on the Register of Critical Infrastructure Assets form *(/resources/online-forms/direct-interest-holder)*.

Examples of events that may require you to provide an update include:

- change in head office location
- divestment of interest in responsible entity
- change in ownership structure
- change in level or nature of interest
- change in ability to influence and control.

Report cyber incidents which impact the delivery of essential services

We strongly encourage all critical infrastructure asset owners to voluntarily report cyber security incidents to the Australian Cyber Security Centre (ACSC) *(https://www.cyber.gov.au/)*. You can report an incident even if it does not meet the threshold for mandatory reporting. Certain responsible entities must also report critical and other cyber security incidents to the ACSC's cyber incident reporting portal *(https://www.cyber.gov.au/report-and-recover/report/report-a-cyber-security-incident#no-back)*.

A cyber security incident is one or more acts, events or circumstances involving one or more of the following:

- unauthorised access to or modification of computer data or a computer program
- unauthorised impairment of electronic communications to or from a computer
- unauthorised impairment of the availability, reliability, security or operation of computer data, a computer program or a computer.

If you become aware that a critical cyber security incident has occurred, or is occurring, you must notify the ACSC. How quickly you need to notify them will depend on the impact of the incident:

- If the incident has had, or is having, a 'significant impact' on the availability of your asset, you must notify the ACSC orally or in writing within 12 hours after you become aware of the incident.
- If the incident has had, is having, or is likely to have, a 'relevant impact' on your asset you must notify the ACSC orally or in writing within 72 hours after you become aware of the incident.

If you report an incident orally, you must also submit a written report within a particular time frame, depending on the impact of the incident:

- You have 84 hours to submit a written report for an incident that has a significant impact
- You have 48 hours to submit a written report for an incident that has a relevant impact.

You must submit this through the ACSC's cyber incident reporting portal *(https://www.cyber.gov.au/report-and-recover/report/report-a-cyber-security-incident#no-back)*.

A significant impact is one where both:

- the critical infrastructure asset is used in connection with the provision of essential goods and services
- the incident has materially disrupted the availability of the essential goods or services delivered by a critical infrastructure asset.

A relevant impact is an impact on the availability, integrity, reliability or confidentiality of your asset.

Reporting an incident:

- If there is a threat to life or risk of harm, call 000 immediately.
- To make an urgent oral report, call 1300Cyber1 (1300 292 371).
- To make a written report, go to the ACSC's website to Report a cyber security incident *(https://www.cyber.gov.au/report-and-recover/report/report-a-cyber-security-incident#no-back)*.

Only some asset classes are required to submit a report. You can find the list of asset classes that are required to submit a report in section 5 of the SOCI (Application) Rules (LIN 22/026) 2022 *(https://www.legislation.gov.au/Series/F2022L00562)*. Failing to report an incident for one of these asset classes may result in a civil penalty or fine.

We encourage all critical infrastructure sectors and assets to voluntarily report cyber incidents, even if:

- your asset does not fall under one of these asset classes
- you aren't sure if the incident is a significant or relevant incident.

You may also have other reporting requirements under other legislation or regulations.

You can read more about this obligation in the Cyber Security Incident Reporting Factsheet (568KB PDF) *(/resources-subsite/Documents/cyber-security-incident-reporting.pdf)*.

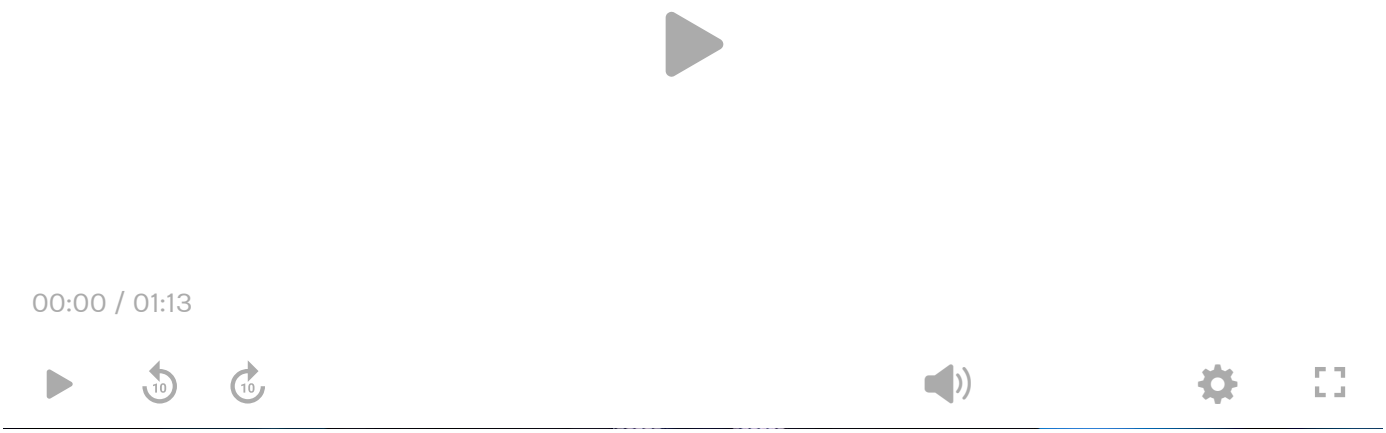
You can read more about how to submit a report in the Mandatory Cyber Incident Reporting Guide (297KB PDF) *(/resources-subsite/Documents/mcir-guidance.pdf)*.

Adopt, maintain and comply with a written risk management program

You may be required to establish, maintain, and comply with a written critical infrastructure risk management program (CIRMP) for your asset. This should identify, and as far as is reasonably practicable, take steps to minimise or eliminate the 'material risks' that could have a 'relevant impact' on the asset.

Critical Infrastructure Risk Management Program Rules – Commenced on 17

February 2023



See transcript

Hi everyone,

The grace period for the Critical Infrastructure Risk Management Program obligation has now ended.

If it applies to you, owners and operators of critical infrastructure entities must now have developed, and implemented, a Risk Management Program.

You have until the 18th of August 2024 to meet the requirements of the cyber security framework identified in the Risk Management Program.

You must then submit a first Board-approved annual report no later than the 28th of September 2024.

Complying with the Critical Infrastructure Risk Management Program obligation will assist in managing the material risks that a hazard might have on your asset.

Once identified, a responsible entity must then eliminate or minimise that hazard occurring, and put mitigations in place.

Now that the grace period has ended, wherever your business is at in terms of its maturity, we're still here to help.

We have for example, extensive guidance available on our website, and you can get in touch with us directly using the contact details on the screen.

Together, we can continue to protect Australia's critical infrastructure… now, and into the future.

> The CIRMP rules commenced on 17 February 2023. Responsible entities must comply with the cyber security framework identified in their written CIRMP by 18 August 2024.

The CIRMP rules were informed by an extensive consultation process. The Minister for Home Affairs made changes to the CIRMP rules to reflect feedback received through this consultation process. We would like to thank all stakeholders who took the time to prepare a submission or otherwise engage with us.

Responsible entities for the following critical infrastructure assets classes are required to adopt, maintain and comply with a written CIRMP:

- Broadcasting
- Domain Name Systems
- Data storage or processing
- Electricity
- Energy market operator
- Gas
- Liquid fuels
- Payment systems
- Food and grocery
- Designated hospitals
- Freight infrastructure
- Freight services
- Water

If your asset becomes a critical infrastructure asset, you must create a CIRMP that complies with this obligation within 6 months of the day the asset became a CI asset.

The responsible entity for the critical infrastructure asset must have and comply with a CIRMP. The purpose of the CIRMP is to:

- identify each hazard where there is a material risk that, if the hazard happened, there would be an impact on the asset
- minimise or eliminate any material risk of such a hazard occurring
- minimise the impact of such a hazard on the asset.

You can find the definition of material risk in section 6 of the CIRMP Rules *(https://www.legislation.gov.au/Series/F2023L00112)*.

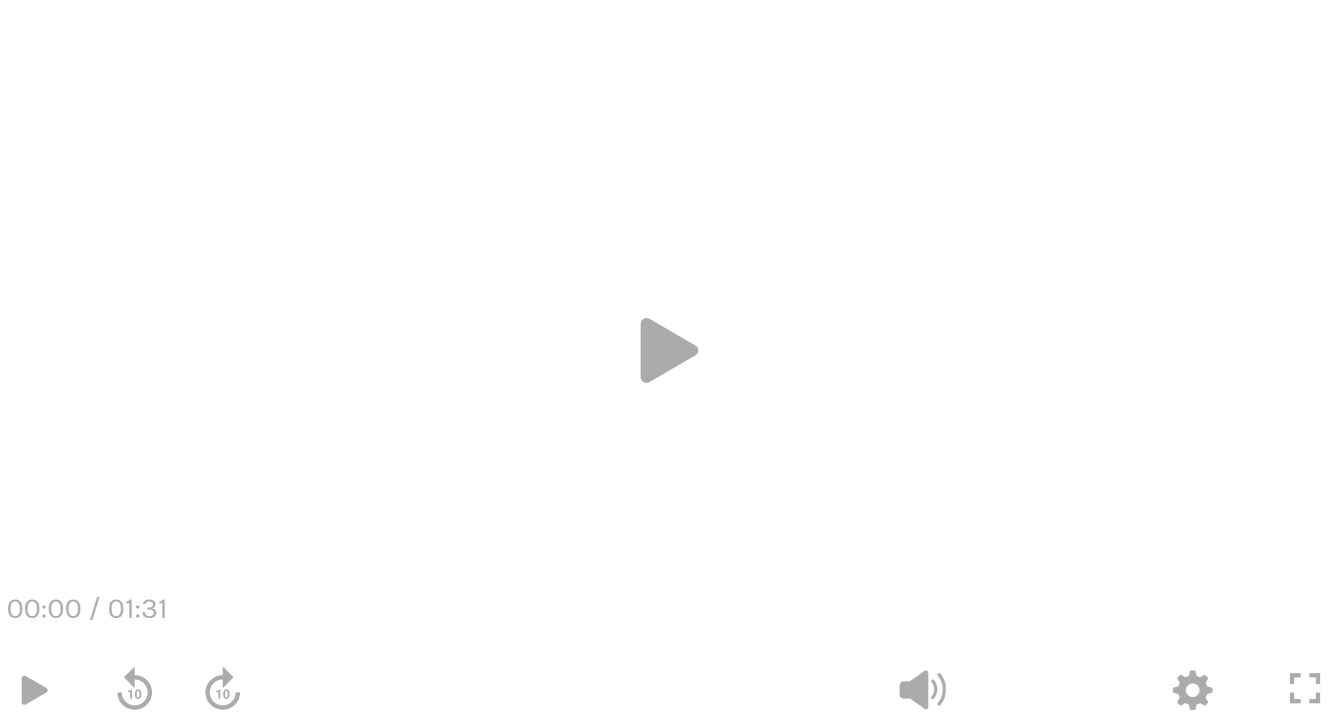
The kinds of hazards that you must identify in your CIRMP include:

- physical security hazards
- natural hazards
- cyber and information security hazards
- personnel hazards
- supply chain hazards.

We recognise that industry is best placed to identify hazards and determine how to minimise or eliminate material risks.

Responsible entities have broad discretion in how they approach the management of hazards which pose material risks to their critical infrastructure asset. Where possible, we are committed to working with you to assist in complying with the CIRMP obligation.

Compliance with the obligation



See transcript

In an increasingly complex and interconnected world, full of unprecedented global threats, Australia's critical infrastructure must grapple with a number of risks.
Including, environmental hazards, cyber incidents, personnel and physical security risks and supply chain disruption.
The Critical Infrastructure Risk Management Program - or CIRMP- is a key measure that will support the ongoing resilience of Australia's critical infrastructure.
Under the CIRMP, critical infrastructure owners and operators are required to identify the risks and hazards that might have an impact on their asset.
The responsible entity must then, so far as it's reasonably practicable to do so, take steps to minimise or eliminate that risk- for example, an entity may consider installing fire suppression systems, or regularly patching networks with the latest software and hardware.

We know industry is best placed to identify the most relevant hazards; that's why the CIRMP Rules are principles-based and allow for broad discretion in how you approach the management of hazards.
We're here to help. If you have any questions about the CIRMP Rules visit the Cyber and Infrastructure Security Centre's website.
Together, we can continue to protect Australia's critical infrastructure; here, now and into the future.

We are the regulator for the CIRMP obligation for all asset classes except payment systems. Payment systems are regulated by the Reserve Bank of Australia. For further information on requirements for this asset class visit the Reserve Bank of Australia website *(https://www.rba.gov.au/)*.

If you would like to arrange a meeting to discuss the CIRMP obligation, contact enquiries@homeaffairs.gov.au *(mailto:enquiries@homeaffairs.gov.au)*.

For a general overview of setting up your risk management program, read the CISC Fact Sheet – Risk Management Program (223KB PDF) *(/resources-subsite/Documents/cisc-factsheet-risk-management-program.pdf)*.

For a detailed overview of setting up your risk management program, read the Guidance for the Critical Infrastructure Risk Management Program (1074KB PDF) *(/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf)*.

Annual reporting

You must provide us with an annual report about your CIRMP within 90 days after the end of the financial year. You must submit the report to a relevant Commonwealth regulator or the Secretary of the Department of Home Affairs using the approved form *(/resources/online-forms/responsible-entity-risk-management-program-annual-report)*.

Responsible entities for critical infrastructure assets subject to the CIRMP obligation must submit an annual report that has been approved by their board, council, or other governing body to the relevant regulator. The annual report will provide assurance that a CIRMP is in place and that the entity is taking steps to manage material risks posed by the hazard to the critical infrastructure asset. If an entity is a responsible entity for a CI asset for **all or part** of the Australian financial year, they will be required to submit an annual report.

Annual reports will help us better understand the threat environment in each sector. This helps government provide meaningful assistance if subject to a hazard, and advise entities on ways to further enhance the security and resilience of critical infrastructure assets.

The SOCI Act requires the annual report to be in an approved form and to include:

- a declaration that the CIRMP is up-to-date at the end of the Australian financial year
- whether a hazard occurred that had a significant or relevant impact on an asset during the year

- whether any variations to the CIRMP were made during the year
- whether the program was effective in mitigating any significant or relevant impact that a hazard may have had on an asset during the year
- an attestation that the information contained within the annual report was approved by the board or governing body of the entity.

The report does not need to contain the full risk management program.

There are penalties for failing to create and comply with a CIRMP, and for failing to submit an annual report. You can find out what penalties are for specific breaches in the SOCI Act *(https://www.legislation.gov.au/Series/C2018A00029)*.

The first annual report required under the CIRMP Rules is for the 2023-2024 Australian financial year. It must be submitted between 30 June 2024 and 28 September 2024.

We also encourage you to voluntarily submit an annual report for the 2022-2023 Australian financial year. This report should provide a 'pulse-check' on how you are implementing the CIRMP. We do not expect this voluntary report to be overly complex or detailed. Rather, it provides an opportunity to reflect on progress in enhancing risk management procedures.