Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Risk Management Program
Frequently Asked Questions

This document answers a number of frequently asked questions we have received as part of our ongoing consultation on the Risk Management Program.

It will be updated on a regular basis throughout the consultation period.

Questions are listed under the following themes:

- Timeframes
- Definitions
- Costings
- Reporting
- Risk Management In Practice
- Cyber Frameworks
- Personnel Hazards And AusCheck
- Supply Chain Hazards

If your question is not answered here, please send it via email to:
CI.reforms@homeaffairs.gov.au

TIMEFRAMES

How long is the consultation process for the Risk Management Program Rules?

Consultation will be conducted over a 45 day period. This is longer than the 28 days mandated by the *Security of Critical infrastructure Act 2018* (SOCI Act). Consultation will close at 5:00pm AEDT on Friday 18 November 2022.

How long until industry has to comply with the Risk Management Program obligations?

There will be a **6 month grace period** for material risk identification and mitigation, and to develop your written risk management program. This 6 month period will begin once the Minister has signed the Rules Instrument.

An **additional 12 month grace period** will apply for the compliance with the cyber security framework you have identified in your written risk management program.

If an entity is unable to meet the new cyber security standard/framework within 12 month reporting period, will there be any penalties applied to the entity?

The Department does not intend to take a punitive approach to entities who are making good faith efforts to comply with their obligations under the SOCI Act. If this occurs, the Department intends to engage in an open dialogue on any issues faced by the responsible entity.

DEFINITIONS

When is a risk a 'material risk'?

While responsible entities should take a broad approach to identifying material risk, the RMP Rules provide instances of material risks that must be considered in the development of your written risk management program. Namely risks that:

- Impact Australia's social or economic stability, defence, or national security;
- Will result in major interruptions to the asset's function;
- Result in substantive loss of access to, or the manipulation of a critical component of the asset;
- Are introduced due to the storage, transmission or processing of sensitive operational information outside Australia;
- Result from remote access or interference with critical operational and information technology systems; or
- Arise from other material risks identified by the responsible entity as affecting the functioning of the asset.

Responsible entities are responsible for determining if a risk is a material risk and should consider the likelihood of a hazard occurring, and the relevant impact on the asset or a critical component of the asset if a hazard were to occur.

What does 'so far as it is reasonably practicable' mean?

Responsible entities within the operating context of their business will need to consider what is 'practicable' for their business. 'So far as it is reasonably practicable' allows entities an opportunity to determine how they address material risk and relevant impact in relation to their business size, maturity and income.

For example, the RMP Rules do not contemplate that a small business compared with a large business will undertake the same measures to consider minimising or eliminating material risk, due to their differing operational context.

Details as to what is expected from a responsible entity by the term 'reasonably practicable' are covered in the explanatory memorandum to the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*. This can be found on the APH website at: Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022.

What constitutes sensitive operational information, as found in section 5(e) of the draft RMP Rules?

While a definition of operational information may be found in the SOCI Act 2018, sensitive operational information has not been defined due

to its specificity to your critical infrastructure, sector, asset, and you as a responsible entity. As the implementation of the Risk Management Program will be principles-based, it is anticipated that each business is best placed to understand what constitutes sensitive operational information as it relates to the delivery of their essential good or service.

COSTINGS

How are you able to demonstrate that the benefits of this obligation outweigh the costs?

The CISC has undertaken a regulation impact assessment with 12 of the 13 sectors on these draft rules – with average costs across all sectors for the first year, and for subsequent years provided in information shared by the Department to the Parliamentary Joint Committee on Security and Intelligence (PJCIS) in their review of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*, and in the explanatory memorandum to that Bill.

The Department is currently working with the food and grocery sector to understand the costs to their business when implementing these rules.

A final regulatory impact assessment will be made publically available with the rules, should the Minister choose to makes them.

Will the regulatory impact statement be revised based on feedback received through the consultation period and the final rules that are signed off?

Should the final rules made by the Minister be substantially different from those currently being consulted on or additional requirements be applied, the Department will reconsider the regulatory impact of the rules.

For any new Rule/s made, a regulation impact statement will need to be prepared for that point in time. A new regulation impact statement does not need to be prepared each time that a framework listed in the Rule is updated, as this is provided for in the Rules and the primary legislation.

What Government funds are available for businesses to implement these critical infrastructure reforms?

At this stage the Government does not intend to provide funding to entities to implement and comply with the reforms specifically under the SOCI Act reforms. The CISC has not been provided with any funding to assist industry.

REPORTING

Which financial year is applied with regards to the reporting requirements?

The Australian financial year, ending on June 30.

Who will be my regulator?

The CISC will be the regulator for 12 of the 13 asset classes currently proposed to comply with the RMP rules.

The Reserve Bank of Australia (RBA) will be the regulator for the payment systems assets.

The annual report includes a section requiring us to describe our asset covered by the RMP - we have already been obliged to provide this information as part of our CI registration - why does the Department want us to provide this information again?

Provision of this information allows us to understand which critical infrastructure assets have complied with obligations. As an entity, you may choose to simply provide the Register of Critical Infrastructure Asset IDs in this box if you are also required to comply with the Register obligation.

If the rules are switched on prior to 31 Dec 2022, with the 6 months grace period given, are Boards required to complete the annual report as at 30 Jun 2023 (recognizing the 90 days post FY submission deadline)?

The CISC understands that in this example, there would only have been a few weeks where the

RMP was operational for entities before the end of the 2023 financial year. Under this example an annual report would be required, however, the CISC would not expect to see copious amounts of information in that report.

This first annual report would be important for providing assurance to an entity's board, and to the CISC, that there is an RMP in place and that the entity is working towards implementing a cyber security framework.

Think of it as a six-month pulse check.

If there are multiple responsible entities of the same asset, does each of the responsible entities have the separate obligation to report the same security incident? This goes the same for the RMPs. Does each of the responsible entities have to establish separate RMPs and produce an annual report separately for the same/single asset?

A critical infrastructure asset should only have one responsible entity, but may have multiple direct interest holders.

The *Security of Critical Infrastructure Act 2018* (SOCI Act) provides definitions for the responsible entity (section 12L) and direct interest holder (section 8). Subsection 12L (420) of the revised explanatory memorandum of the *Security Legislation Amendment (Critical infrastructure) Bill 2021* states that a responsible entity is that entity with ultimate operational responsibility of the asset.

Section 5 of the SOCI Act defines interest in an asset to mean a legal or equitable interest in the asset. Entities which meet either or both of 8(1)(a), 8(1)(b) are direct interest holders, and may have reporting requirements for the Register of Critical Infrastructure Assets obligation.

Please note that **only** the responsible entity for a critical infrastructure asset is required to maintain a risk management program under the RMP obligation.

RISK MANAGEMENT IN PRACTICE

What should entities prioritise when considering their risk process and development of the RMP?

The RMP is a great opportunity for owners and operators to 'think big' and take an 'all hazards' approach to safeguarding their business, assets, and people.

Risk management is context specific across all the asset classes and threat vectors, so we recognise that entities are best placed to make determinations that they feel appropriately reflects their operational context.

Throughout this process, we are trying to support your capability to manage risks, not enforce an arbitrary compliance regime.

Entities are strongly encouraged to join the *Trusted Information Sharing Network*, it is a fantastic source of support and information for critical infrastructure entities.

Contact cir@homeaffairs.gov.au to learn more about how to join the TISN

The draft RMP rules ask entities to describe interdependencies between their assets and other critical infrastructure assets. Could you please provide additional guidance on this requirement?

This obligation is asking entities to identify where there are specific interdependencies that are critical to the ability of their asset to operate. In terms of compliance, CISC is wanting entities to think holistically about the key risks posed by their dependencies on other assets, rather than meticulously cataloguing every utility and supplier with which their asset/s interacts.

Is there a standard template to be used for the risk management process required by the Government?

No. As the Rules are principles-based, there is no set or defined template required for the risk assessment. You may develop a critical

infrastructure risk management program in the format that is suitable for your business and its operational needs.

The Department is open to working with entities to develop a standard form for the risk management program if that is of interest.

How does CISC expect responsible entities to determine the likelihood of threats/hazards?

Likelihood is fundamentally a qualitative assessment made by a responsible entity based on their circumstances and understanding of the possibility that a foreseen outcome may occur. To assist, the CISC has recently published *Sector Risk Assessment Advisories* for all critical infrastructure sectors (other than Defence) which can act as a good starting point for entities in this process.

However, fundamentally the CISC is not being overly prescriptive as to what a likely material risk is for each entity or how likely it is to occur. Responsible entities are best placed to make that assessment for their business, including whether mitigations are appropriate. CISC will provide overarching guidance on key risks, but these should not be the totality of what is considered.

What is the relationship between the new Critical Infrastructure Uplift Program from the Australian Cyber Security Centre, and the Risk Management Program rules?

A: “The CI-UP program offers a range of scaled and tailored services to Critical Infrastructure Partners. CI-UP aims to uplift and harden the cyber defences of CI Partner entities, with a focus on operational technology and OT/IT interfaces through an intelligence led understanding of risks. CI-UP is not a compliance or audit exercise and is not designed to assist organisations to meet their regulatory requirements set out in the RMP. Entities interested in the CI-UP can read more about the program on the ACSC website.”

In regards to Section 7(2)(f) of the Draft RMP Rules, is the responsible entity required to identify every single position of every individual who contributes in some way to the development, implementation and ongoing management of the RMP?

No, the responsible entity does not need to list every employee who is involved in mitigating a risk. Responsible entities are required to identify the primary positions who are responsible for the development and review of the RMP document. The intention of this requirement is to encourage an internally unified approach to risk management within responsible entities.

CYBER FRAMEWORKS

I have my own cybersecurity policies in place. Do I still have to comply with one of the frameworks specified in the RMP Rules?

The rules require you to comply with a framework/standard including any conditions, to ensure that there is a baseline level of cybersecurity across all critical infrastructure assets.

If the policies you already follow are equivalent to the framework/standard outlined in the draft rules then that should be sufficient.

What constitutes ‘an equivalent framework’?

Equivalent frameworks must at least meet the cyber security protections provided by the specified frameworks/ standards.

Responsible entities should be able to justify to their board, council or other governing body that the cybersecurity framework/standard chosen meets or exceeds the level of cybersecurity protection afforded by the frameworks/standards outlined in section 7(4)(b) of the RMP Rules.

The CISC recommends that any framework or standard chosen should be endorsed by a government (such as with the United States Cybersecurity Capability Maturity Model) or international organisation (such as the International Organisation for Standardisation).

The CISC recommends responsible entities justify their equivalency in their RMP.

What do I need to do if the cyber security framework we have in our RMP is updated or changes?

Cyber security frameworks and the requirements under them will change over time as the cyber security environment evolves.

Entities will be expected to move to the most current version of the framework/standard they have identified in their RMP to ensure they keep pace with the hazards they are facing.

Part 2A prescribes a number of cyber frameworks that are a mix of controls frameworks and maturity frameworks but my preferred framework isn't listed. Could this be added to the list of preferred frameworks?

The list of frameworks is intended to provide options to responsible entities with a varied selection of options for managing their risks. This list has been developed through consultation, and is not meant to be exhaustive.

If an entity chooses to adopt an equivalent framework that the company board, or governing body, agrees to utilise, this should meet their obligation to manage the risk to their asset.

It is noted that these listed frameworks go to cyber and information security, which may include both IT and OT. Frameworks that do not directly address these aspects of a critical infrastructure asset would not be considered equivalent.

PERSONNEL HAZARDS AND AUSCHECK

Am I required to have an ongoing background checking system for critical workers?

It is a requirement under section 9(2) that entities must have a process or system to identify critical workers and assess their suitability on an **ongoing basis**. Furthermore, entities must minimise or eliminate risks posed by incoming, ongoing and outgoing employees and contractors.

A responsible entity may consider that an AusCheck or another type of ongoing background check is the most appropriate process to meet this requirement.

Is an AusCheck mandatory under the RMP?

No, it is **not mandatory**.

An AusCheck is an optional check that an entity could use as **one element** in the process of satisfying their board, or governing body that they are complying with requirement under the RMP.

What is a 'critical worker'?

A critical worker is defined in section 5 of the SOCI Act as an individual, who is an employee, intern, contractor or subcontractor of the responsible entity for a critical infrastructure asset whose absence or compromise would prevent the proper function of the asset or could cause significant damage to the asset, as assessed by the entity, and the individual has access to, or control and management of, a critical component of an asset.

In practice, this could include roles such as Chief Information Security Officer or Control Room Operator or workers such as IT administrators with full and unrestricted administrator rights and access to the systems (sometimes referred to as 'god-mode' or 'unlimited' access).

The CISC believes that entities are best placed to understand the criticality of their operations and employees. Businesses will be ultimately responsible for determining their critical workers.

What are the benefits of an AusCheck background check?

The benefits of an AusCheck background check are that it provides an accountable process which is transparent about:

- An established, standard process for all
- A unique assessment that considers national security
- Assessments of criminal history based on national risk
- Protection of applicants' rights
- A cyber-secure and efficient process

What is the difference between an AusCheck background check and other available background checks?

AusCheck is the only background checking provider that has the ability to utilise an ASIO security risk assessment.

For more information on the AusCheck background checks, please visit the AusCheck website.

Is there a specific AusCheck for critical infrastructure sectors?

The intention is to form a new type of ongoing check under the AusCheck scheme.

The AusCheck Framework provided in this consultation period can provide more detail and the Department is happy to discuss any queries or concerns with the proposed framework for background checks for Critical Infrastructure.

What sort of cost would be involved for conducting an AusCheck background check?

This decision is still pending, subject to the consultation currently being undertaken.

Currently, the AusCheck background checking fees are $92.50 excluding GST and $100.35 excluding GST for a background check including an immigration and citizenship check.

Please note: these fees are subject to review.

What is the timeframe to get results back from AusCheck?

On average AusCheck finalises 80% of background checks within 2 weeks of receiving the application.

Will I be able to do AusCheck during the six month grace period before the written risk management program must be established?

Yes.

AusCheck background checks will be available from when the RMP obligations are switched on and the AusCheck Regulations are amended.

Is the Department confident that changes to the AusCheck scheme will be in place before the rules come into force?

The AusCheck Regulations are required to be amended prior to the RMP Rules coming into force. The CISC will communicate to industry once this occurs.

Are companies able to use other background checking schemes that they might already use for the mitigations for personnel hazards?

Yes.

There is no requirement to use AusCheck under the draft RMP Rules.

How will AusCheck background check a foreign worker?

As part of the AusCheck background checking process, ‘critical workers’ will be subject to a ‘right to work in Australia’ check if they are an Australian Visa holder. This check is conducted through the Department of Home Affairs’ Visa Entitlement Verification Online (VEVO) system.

Can an AusCheck background check be used for critical workers located overseas?

An AusCheck background check is a "point-in-time" check at present, with an assessment of a person in an Australian-based context (for example - the person's identity within Australia needs to be established; a person's criminal history in Australia). It is up to each responsible entity to determine if an AusCheck background check is a suitable risk mitigation for their critical workers, depending on the risks and the critical worker's circumstances.

How long is an AusCheck background check valid? How frequently are checks required?

It is up to the responsible entity to determine the frequency of any hazard mitigations. This includes

mitigations for personnel security risks, such as whether to use an AusCheck background check, and the renewal period for any checks.

The AusCheck background check is a “point-in-time” assessment, using information from the day of the application. There is no set validity period for the AusCheck background check proposed for critical infrastructure, and no specified cadence by which a responsible entity can request a further checks.

SUPPLY CHAIN HAZARDS

How far down a supply chain do I have to consider?

It is the responsibility of each entity to determine how ‘far down’ the supply chain it chooses to consider relevant when determining supply chain hazards.

Responsible entities should consider the likely relevant impact a business may have on the entity’s operational function and risk to supply chain when deciding how far down a supply chain to consider.

The Department encourages responsible entities to have collaborative discussions with their relevant goods and services providers regarding plans to manage risk and potential impact on the supplier.