Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Risk Management Program

The Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) amends the *Security of Critical Infrastructure Act 2018* (SOCI Act) to build upon the existing framework and uplift the security and resilience of Australia's critical infrastructure.

What is a risk management program?

The risk management program is a **written program** that applies to responsible entities for one or more critical infrastructure assets.

Responsible entities must identify, and as far as is reasonably practicable, take steps to minimise or eliminate **'material risks**' that could have a '**relevant impact**' on the asset.

The risk management program is intended to uplift core security practices that relate to the management of critical infrastructure assets. It aims to ensure responsible entities take a holistic and proactive approach toward identifying, preventing and mitigating risks from all hazards.

What are the risk management program obligations?

Responsible entities are required to establish, maintain, and comply with a risk management program to manage the 'material risk' of a 'hazard' occurring, which could have a relevant impact on the critical infrastructure asset. The *Security of Critical Infrastructure (Critical Infrastructure risk management program) Rules (LIN 22/018) 2022* (Risk Management Program Rules) will specify the matters to be contained in a risk management program, and will require a responsible entity to meet the following principles-based outcomes:

Identify material risks – Entities will have a responsibility to take an all-hazards approach when identifying hazards that may affect the **availability**, **integrity**, **reliability** and **confidentiality** of their critical infrastructure asset.

Minimise risks to prevent incidents – Entities will be required to consider risks to their critical infrastructure asset and establish appropriate strategies to minimise or eliminate the risk of hazards occurring, so 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.

Strategies could include enhanced cyber security controls, background checking of critical worker, having back-ups of key systems, ensuring adequate stock on hand in case of a disruption, installing redundancies for key inputs, out-of-hours processes and procedures, and the ability to communicate with affected customers, clients and agencies.

Mitigate the impact of realised incidents – Entities will be required to have robust procedures in place to mitigate, so far as is reasonably practicable, the impacts of a hazard, as well as work to recover as quickly as possible.

Effective governance – Through the risk management program and risk management program rules, entities will be required to have appropriate risk management oversight arrangements in place, including evaluation and testing. Compliance would be assessed by the relevant regulator, noting that what is appropriate would be unique to each entity.

What assets are affected by the obligations?

The risk management program rules are proposed to apply to the following critical infrastructure assets in the first instance:

- Critical broadcasting assets
- Critical domain name system
- Critical data storage or processing assets
- Critical hospitals
- Critical energy market operator assets
- Critical water assets
- Critical electricity assets
- Critical gas assets
- Critical liquid fuel assets
- Critical financial market infrastructure assets that are specified payment systems operator assets
- Specified critical defence industry assets

The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.

What is a 'material risk', relevant 'impact' and 'hazard'?

Material risk

A **'material risk'** to a critical infrastructure asset includes the risk of impairment, stoppage, loss of access to or interference with the asset. It also includes a risk to the asset of the impact resulting from sending information outside Australia and a risk associated with remote access to the asset.

Entities will have a responsibility to take an 'all-hazards' approach when identifying these risks and must have regard of the **likelihood of a hazard occurring** and **relevant impact of** the **hazard on an asset** if the hazard were to occur.

Hazards in the rules

At present the proposed rules contain obligations relating to protections within four key hazard vectors:

- **Physical and natural** – the physical risks to parts of the asset critical to the functioning of the asset, such as physical access to sensitive facilities or 'control rooms', or natural disasters.
- **Cyber and information security** – the 'cyber' risks to the digital systems, computers, datasets, and networks that underpin critical infrastructure systems.
- **Personnel** – the 'trusted insider' risk posed by critical workers who have the access and ability to disrupt the functioning of the asset.
- **Supply chain** – the risk of disruption, malicious or otherwise, or exploitation of critical supply chains leading to a disruption of the critical infrastructure asset.

Relevant impact

A **'relevant impact'** is an impact on the availability, integrity, and reliability of the asset, and the impact on the confidentiality of information about the asset, information stored in the asset if any, and, if the asset is computer data, the computer data.

The relevant impact may be direct or indirect. It must be more serious than a reduction in the quality of service being provided.

What are the risk management program rules?

The risk management program rules contain the requirements of the risk management program and have been developed with industry through extensive consultation. They set out the principles based requirements for responsible entities to mitigate and minimise risks within the four domains. Following amendments made by the SLACIP Act, the Minister for Home Affairs may choose to make these rules. Before this occurs, the Minister must publish a notice on the Department's website, setting out the draft risk management program rules and inviting submissions about the rules for a minimum of 28 days. The Minister must consider all submissions received within the period specified in the notice.

More detailed guidance material will be developed to assist responsible entities discharge their risk management program obligations under the risk management program rules.

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

The requirement to minimise or eliminate material risks **'so far as it is reasonably practicable'** seeks for responsible entities to do what was at a particular time, reasonably able to be done to address those risks.

In considering the material risks to their business, responsible entities must weigh up what can be done to mitigate those risks- i.e. what is possible in the circumstances, with whether those actions are reasonable in the circumstance. There is no expectation that entities pursue risk mitigation measures that are disproportionate relative to the likelihood and consequences of a particular risk.

The requirement provides responsible entities flexibility to determine how they address material risk and relevant impact in relation to their business size, maturity and income. The intent is for responsible entities to seek to minimise or eliminate material risk where it is reasonably able to do so, in order to secure their critical infrastructure asset.

In the annual attestation the Board, council or other governing body (if they have one) are required to approve the risk management plan and in doing so, appropriately balance the costs of risk mitigation measures with the impact of those measures in reducing material risk within their own operational context.

The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.

What are the annual reporting requirements?

Entities will be required to provide an **annual report** to the relevant Commonwealth regulator or the Secretary of the Department of Home Affairs, regarding the risk management program. Entities must submit this report within **90 days** after the end of the financial year and the report must be approved by the entity's board, council, or other governing body.

The report must be in the approved form (currently under development and industry consultation is planned) and state whether the risk management program was up to date, any variations to the program, and details of how the program was effective in mitigating any relevant impacts that hazards may have had on that asset during that year.

The report will be used by the Government to better understand the threat environment in each sector and to provide meaningful assistance and advice to entities on ways to further enhance the security and resilience of critical infrastructure assets.

The report does not need to contain the full risk management program, but must be sufficient to assure the relevant Commonwealth regulator or the Secretary that the program remains up to date and appropriate.

The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document. Further details on copyright and disclaimer is available on the Department of Home Affairs' website: [Copyright and disclaimer for our website (homeaffairs.gov.au)].