Australian Government
Department of Home Affairs

Critical Infrastructure Risk Management Program

Addendum: Enhancement to risk management program rules in response to worsening threat environment

Table of Contents

Executive Summary

This Addendum to the 2022 Regulation Impact Statement: A Risk Management Program Framework for Critical Infrastructure Assets (2022 RIS or OBPR22-02914) assesses whether proposed enhancements to the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 (CIRMP Rules) are justified, proportionate, and effective in addressing identified gaps in current risk management practices.

Critical infrastructure is fundamental to Australia's economic activity, national security, and the delivery of essential services. The increasing interconnectivity of infrastructure systems has improved efficiency and productivity, but has also increased systemic risk. Disruption to a single asset can cascade across sectors, resulting in broader economic and societal impacts.

Since the introduction of the CIRMP Rules, the threat environment has become more complex, persistent, and targeted. Cyber actors are increasingly seeking to establish long-term access to critical infrastructure systems to enable disruption. At the same time, supply chain dependencies, insider threats, physical security vulnerabilities, and emerging technologies have introduced additional risk vectors. These developments have exposed limitations in the consistency and maturity of current risk management practices across sectors.

While the existing CIRMP framework, established under the *Security of Critical Infrastructure Act 2018* (SOCI Act) and amended by the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*, sets out baseline obligations for responsible entities to identify and manage material risks and minimise or eliminate those risks so far as reasonably practicable, implementation maturity varies. Key gaps include inconsistent application of cyber security controls, limited visibility into critical supply chain dependencies, insufficient personnel and physical security governance, and a lack of structured assessment of emerging risks.

The proposed enhancements to the CIRMP Rules introduce targeted, risk-based uplift across key areas of vulnerability. The enhancements have been informed by multiple consultation rounds. The enhancements include: strengthening cyber security maturity and control expectations; improving the identification and management of supply chain risks; and vendor assessments of existing or proposed major suppliers; formalising personnel security and insider threat controls; introducing requirements for structured physical security planning; and requiring assessment of risks arising from emerging technologies.

Maintaining the current settings would avoid additional regulatory burden but would not address identified gaps in risk management practices or reflect the current threat environment. As a result, vulnerabilities would persist, and the likelihood and impact of disruptions to critical infrastructure would remain elevated.

By improving the consistency and maturity of risk management practices, the proposed enhancements are expected to reduce the likelihood and potential impact of disruptions to critical infrastructure. Given the interconnected nature of these assets, even marginal reductions in the probability or severity of disruption are expected to deliver substantial economic and societal benefits.

These benefits are difficult to value precisely because the avoided events are not directly observable. It isn't feasible to identify which cyber intrusions, supply chain compromises, insider incidents, physical security breaches or outages would have occurred without the risk framework. The Addendum, therefore, does not rely on a single monetised benefit estimate. It uses regulatory burden costing, consultation evidence and break-even analysis to test whether the expected benefits are likely to justify the additional costs.

The Addendum does not reopen the policy decision made through the 2022 RIS or the development of the enhanced CIRMP Rules. Its purpose is to explain the incremental impact of the proposed enhancements against the existing CIRMP baseline. It does this by setting out the targeted scope of the enhanced requirements, the regulatory burden estimate (RBE), consultation evidence, break-even analysis, and implementation considerations. This provides a transparent basis for understanding the likely impacts of the enhanced CIRMP Rules, including the areas where costs, feasibility constraints and residual uncertainty will need to be managed through guidance, staged implementation and ongoing engagement with industry.

1. Background

1.1. Issues identified in the critical infrastructure environment

The CIRMP Rules came into effect in 2023 and operationalise the requirements in Part 2A of the SOCI Act. These Rules require responsible entities for certain critical infrastructure assets to establish, maintain and comply with a risk management program that identifies hazards which may give rise to material risks and minimises or mitigates their impact across cyber, physical, personnel and supply chain domains.

Since the establishment of the CIRMP Rules, the threat environment for critical infrastructure has become more severe and more complex. Intelligence indicates an increase in threats across all hazards, including cyber threats, supply chain compromise, foreign interference, and other disruptive activity targeting essential services. Hostile foreign state actors and their proxies are increasingly targeting critical infrastructure globally to gain strategic leverage, disrupt essential services, and position themselves for coercive advantage.[1]

This type of activity, including malicious cyber campaigns, supply chain compromises, manipulation of managed service providers, foreign interference, and vulnerabilities from hidden foreign ownership, control, and influence (FOCI) structures, is increasingly on the rise as many of these tactics are designed to remain undetected and gradually influence operational control. [2]

The Director-General of Security's Annual Threat Assessment 2025 highlighted that nation-state actors are increasingly mapping and targeting critical infrastructure.[3] In 2024, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) joined Five Eyes intelligence partners in publicly attributing the compromise of multiple United States (US) critical infrastructure sectors to a state-sponsored group known as Volt Typhoon.[4]

The Annual Cyber Threat Report 2024-2025 from ASD's ACSC reported that 13% of the over 1,200 cyber incidents in that period were reported by critical infrastructure. This is an increase of 2% from the previous year, with the most common types of cyber security incidents involving compromised assets and networks, compromised accounts and credentials, and Denial of Service (DoS)/Distributed DoS attacks.[5]

Threat actors are not limited to exploiting cyber vulnerabilities. FOCI arrangements within both critical infrastructure entities and throughout supply chains exacerbate cyber risks. [6] Incidents affecting critical infrastructure frequently start in the supply chain.[7] Recent reporting on undeclared communications equipment in foreign-made solar inverters illustrates how cyber, supply chain and physical technology risks can converge in energy infrastructure.[8] [9] The renewable energy transition has identified an over-reliance on high-risk vendors and suppliers due to limited manufacturing options. It is therefore necessary to ensure adequate controls and risk mitigations are implemented.

Espionage has become one of the most significant national security threats to Australia. Recent modelling by the Australian Institute of Criminology (AIC) for the Australian Security Intelligence Organisation (ASIO) in the Cost of Espionage report shows that the costs of this degraded environment could exceed $1 billion per espionage-enabled cyber incident affecting critical infrastructure, regardless of the vector. The same report

---

[1] https://www.asio.gov.au/director-generals-annual-threat-assessment-2025
[2] https://www.homeaffairs.gov.au/nat-security/files/foci-risk-assessment-guidance-without-appendices.pdf
[3] https://www.asio.gov.au/director-generals-annual-threat-assessment-2025

[4] https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/prc-state-sponsored-actors-compromise-and-maintain-persistent-access-us-critical-infrastructure

[5] https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf

[6] https://www.homeaffairs.gov.au/nat-security/files/foci-risk-assessment-guidance-without-appendices.pdf
[7] https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2024.pdf
[8] https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/
[9] https://www.aspistrategist.org.au/its-not-just-software-physical-critical-equipment-cant-be-trusted-either/

indicated that insider threats involving state or state-sponsored actors impacting Australian businesses were estimated to cost up to $324.8 million.[10]

These threats are increasingly focused on critical infrastructure asset classes with the highest potential consequences. At the same time, growing interdependencies across sectors have increased the risk that disruption to one asset may cascade more broadly across the economy and the community.

Operational experience and engagement with industry have also identified increasing risks associated with supply chains, third-party service providers, and ownership and control arrangements. These risks can introduce vulnerabilities that are difficult to detect and manage, particularly when dependencies span jurisdictions or sectors. This has been reinforced through consultation with industry and Government stakeholders, which has highlighted the growing complexity of managing interconnected risks.

While the CIRMP framework established in 2022 has driven an uplift in baseline risk management practices, it was designed as a broad, sector-wide framework. The current threat environment has highlighted that, for some high-risk asset classes, baseline requirements alone may no longer be sufficient.

This has created a need for targeted enhancements to the CIRMP Rules to ensure that responsible entities for those asset classes are managing risks in a way that is proportionate to the consequences of disruption.

1.2. Targeted uplift for high-risk asset classes

The proposed amendments to the CIRMP Rules are intended to increase risk management requirements for asset classes that pose the greatest potential consequences for Australia's national security and economic stability. These amendments align with assessments by the National Intelligence Community (NIC), which have identified sectors and asset classes as at elevated risk. This reflects both the criticality of these assets to the delivery of essential services and their attractiveness as targets for hostile actors.

Under the proposed approach, enhanced CIRMP Rules requirements will apply to nine specified asset classes across four sectors.

Table 1: Specified Asset Classes in scope for enhanced CIRMP obligations

Sector	Asset classes
Energy	Energy market operator assets Electricity assets Gas assets Liquid fuel assets
Communications	Broadcasting assets Domain name systems
Water and sewerage	Water assets
Transport	Freight service assets Freight infrastructure assets

For this Addendum's RBE, the estimate is based on the identified population of the nine specified asset classes. The Departmental administrative data available for impact analysis identifies 627 CIRMP records across the in-scope asset classes as at 2 February 2026. The figures below serve as the basis for the regulatory burden estimate. They should be read as asset-class records or CIRMP population counts, not necessarily as counts of unique corporate groups, since some responsible entities may hold multiple assets or operate across multiple asset classes. The Department has also noted that entities that have not submitted annual attestations, although obligated to do so, are not included in the provided totals.

[10] https://www.aic.gov.au/sites/default/files/2025-08/the_cost_of_espionage.pdf

Table 2: CIRMP population

Sector	In-scope asset class	CIRMP population count
Energy	Energy market operator assets	11
Energy	Electricity assets	348
Energy	Gas assets	87
Energy	Liquid fuel assets	47
Communications	Broadcasting assets	3
Communications	Domain name systems	17
Water and sewerage	Water assets	31
Transport	Freight service assets	56
Transport	Freight infrastructure assets	27
	Total	**627**

Source note: Based on Departmental data provided for impact analysis as at 2 February 2026.

1.3. Alignment with the current regulatory landscape

All asset classes in scope are already required to develop and maintain a CIRMP under Part 2A of the SOCI Act. The proposed enhancements do not introduce a new obligation for these asset classes, but instead strengthen existing requirements to ensure a more consistent and proportionate level of risk management maturity.

This targeted scope is central to the impact analysis. The 2022 RIS costed the full CIRMP framework across a broader set of asset classes. The 2026 enhanced CIRMP package applies only to the asset classes identified as higher risk and higher consequence for this reform. It therefore imposes a smaller incremental regulatory burden than the original CIRMP framework, while targeting the areas where additional risk-management maturity is most needed. The enhancements maintain the CIRMP's existing hazard-domain structure and do not introduce new asset classes. Compliance and assurance will continue to rely primarily on existing CIRMP governance and annual reporting arrangements.

This targeted approach recognises that not all critical infrastructure assets require the same level of enhanced rules under the CIRMP. It is designed to focus effort where it is required, avoiding unnecessary duplication and regulatory burden on other asset classes. In some cases, asset classes not captured by the enhanced CIRMP Rules are subject to alternative regulatory frameworks that impose comparable obligations. This includes asset classes regulated under:

- *Aviation Transport Security Act 2004*
- *Maritime Transport and Offshore Facilities Security Act 2003*
- APRA, specifically Prudential Standard CPS 230 – Operational Risk Management
- Defence Industry Security Program.

The proposed rule enhancements also recognise that responsible entities have obligations under other legislative frameworks that may mirror these obligations, including the *Modern Slavery Act 2018* (Modern Slavery Act), the *Foreign Acquisitions and Takeovers Act 1975*, and the *Corporations Act 2001* (Corporations Act).

2. Options considered and preferred approach

Government has considered three options to address the need for enhanced risk management requirements for in-scope critical infrastructure asset classes. The options have been assessed against the current CIRMP Rules as the business-as-usual baseline. All asset classes in scope are already required to develop, maintain, comply with and annually report on a CIRMP under Part 2A of the SOCI Act. The question considered in this Addendum is therefore whether additional, targeted uplift is justified above the existing CIRMP baseline.

The options are assessed against effectiveness in addressing identified risks, proportionality, direct regulatory burden, implementation feasibility, consistency with the existing CIRMP architecture, consultation feedback and expected net benefit. This approach reflects the incremental nature of the proposed amendments and avoids double-counting the costs of activities already required under the existing CIRMP Rules.

2.1. Option 1: Status quo

Under Option 1, no amendments would be made to the CIRMP Rules. Responsible entities for the nine in-scope asset classes would continue to comply with existing CIRMP requirements, including the obligation to identify, assess and manage material risks across cyber and information security, personnel, supply chain, and physical and natural hazard domains through a written all-hazards risk management program.

Government would continue business-as-usual threat engagement, sector engagement, guidance and regulatory oversight. However, no additional rule-based clarification or uplift would be introduced for the in-scope asset classes.

The existing CIRMP Rules have established a baseline level of risk management maturity and have driven an uplift in risk management practices. However, they were designed as a broad, multi-sector framework and do not provide additional specificity for high-risk asset classes operating in a more complex and interconnected threat environment. Responsible entities would continue to interpret and implement requirements with varying levels of maturity, resulting in inconsistent application of risk management practices across sectors.

Option 1 would avoid any new direct regulatory burden. However, it would not address identified gaps in the consistency, maturity and documentation of risk management practices for high-risk assets. It would also not address the increasing complexity and severity of the threat environment identified through intelligence assessments, operational experience and stakeholder feedback. Maintaining current settings would risk a widening gap between regulatory expectations and the nature of contemporary threats. As a result, this option is not preferred.

2.2. Option 2: Improved awareness

Under Option 2, the CIRMP Rules would remain unchanged, but Government would seek to improve risk management practices through non-regulatory measures. These could include updated guidance, templates, advisory materials, threat briefings, best-practice materials, voluntary uplift pathways and continued engagement through the Trusted Information Sharing Network and other sector forums.

This option would allow responsible entities to adopt improved practices tailored to their operating context voluntarily. It would avoid imposing mandatory new compliance costs on responsible entities, provided the measures remained genuinely voluntary. It would involve some additional cost to Government in developing and delivering guidance and engagement activities.

While this approach may improve awareness and support incremental improvements, its effectiveness would depend on voluntary uptake by responsible entities. Consultation feedback indicates that guidance alone is unlikely to deliver consistent uplift across all in-scope asset classes. Voluntary measures may be adopted unevenly, particularly when implementation involves capital expenditure, legacy operational technology environments, constrained supplier markets, contractor workforces, or investments that require approval through regulated pricing or funding cycles.

Non-regulatory approaches would support awareness and voluntary uplift, but would not deliver consistent, enforceable or auditable improvements across the in-scope asset classes. Variability in capability and risk

prioritisation would likely persist, particularly in sectors with constrained resources or complex operating environments. As a result, this option is not preferred.

2.3. Option 3: Enhanced CIRMP requirements

Consistent with the targeted scope described in Section 1.3, under Option 3, the CIRMP Rules would be amended to introduce targeted enhanced requirements for the nine in-scope asset classes only. The enhancements build on the existing CIRMP framework rather than creating a new regulatory model. They clarify and strengthen how responsible entities for in-scope assets must identify, assess, document, govern and manage material risks in areas where the existing framework has not produced sufficiently consistent maturity.

Option 3 does not expand the CIRMP to new asset classes and does not apply enhanced obligations to all asset classes subject to the existing CIRMP. Responsible entities for in-scope assets would remain subject to existing baseline CIRMP obligations and also to enhanced requirements. The enhanced requirements would prevail to the extent of any inconsistency.

The Exposure Draft gives effect to this option through enhanced requirements in sections 6A, 8A, 8B, 8C, 9A, 10A and 11A. The final policy position has been refined following consultation. The previously consulted specified-risk-advice workflow is not treated as a standalone final measure. The remaining measures can be implemented in a risk-based manner and supported by guidance, implementation planning and proportional assurance.

Option 3 provides a clearer and more enforceable basis for uplift in high-risk asset classes while maintaining flexibility for responsible entities to tailor controls to asset criticality, operational context, legacy systems, supplier constraints and existing risk-management arrangements. It also provides pricing regulators with a clearer indication of the required uplift, which may support funding and cost-recovery decisions in economically regulated sectors.

Table 3: Enhanced requirements under Option 3

Draft rule section	Hazard Enhancement	Description
Section 4A	Application of enhanced CIRMP requirements	Identifies the specified asset classes to which the enhanced requirements apply and clarifies the relationship between baseline and enhanced CIRMP obligations.
Section 6A	Enhanced material risks	Requires responsible entities to consider material risks relating to impairment of asset functions affecting social stability, economic stability, national security or defence, and compromise or impairment connected with FOCI.
Section 8A	Cyber and information security hazards	Requires processes or systems to address specified cyber material risks and comply with listed cyber frameworks and applicable conditions or an equivalent framework.
Section 8B	Credential compromise hazard	Requires processes or systems to be implemented that achieve phishing-resistant MFA.
Section 8C	Computer lateral movement hazard	Requires processes or systems to be implemented that identify, segregate, recover and restore critical systems.
Section 9A	Personnel hazards	Requires processes or systems for personnel access management, critical worker suitability assessment, ongoing monitoring, incoming and outgoing critical worker risks, and AusCheck or equivalent arrangements for critical workers with access to critical components.

Draft rule section	Hazard Enhancement	Description
Section 10A	Supply chain hazards	Requires processes or systems to map major suppliers and critical components across their supply chains, identify vulnerabilities and maximum tolerable outage, and assess risks associated with existing or proposed major suppliers.
Section 11A	Physical security and natural hazards	Requires processes or systems to centrally manage physical security and natural hazards, including physical security consequences arising from cyber, lateral movement, credential compromise, personnel, supply chain or other hazards, and to outline site characteristics, critical components, sensitive areas, access controls, surveillance, alarms and response measures.

In practice, this option is expected to yield a more consistent and mature risk management approach across critical infrastructure asset classes. Responsible entities may incur additional costs associated with developing more structured processes, improving documentation, enhancing governance arrangements and implementing targeted controls. Consistent with the 2022 RIS, the cost impacts of CIRMP obligations are justified where they are outweighed by the avoided costs of disruption and the resilience benefits of improved risk management.

2.4. Regulatory burden and expected net benefit by option

The RBE comparison is summarised below. Detailed methodology, assumptions and sensitivity testing are set out in Section 3 and Appendix A.

For the purposes of the regulatory burden estimate, Options 1 and 2 have nil direct additional regulatory burden. Option 1 does not change existing regulatory requirements. Option 2 relies on voluntary guidance and engagement and therefore does not impose new mandatory obligations, provided it remains genuinely non-regulatory. This does not mean these options have no economic cost. Under Option 1, the cost is continued exposure to disruption risk and uneven risk maturity. Under Option 2, entities may voluntarily incur costs in response to guidance. Still, voluntary costs are not counted in the regulatory burden estimate unless the policy effectively requires regulated entities to act.

Option 3 has a central estimate of $57.5 million per year in average annual business regulatory burden. The central estimate applies a 10 per cent incremental uplift to the 2022 RIS average annual cost base for the asset classes now in scope of the enhanced CIRMP Rules. The low and high estimates apply 5 per cent and 15 per cent uplifts, respectively. These assumptions are not presented as a statistical confidence interval. They are transparent sensitivity scenarios designed to test the plausible incremental burden of the enhanced obligations against the best available reference-class cost base.

Table 4: Regulatory burden estimate by option

Average annual regulatory costs from business as usual	Business	Community organisations	Individuals	Total
Option 1: Status quo	$0.0m	$0.0m	$0.0m	$0.0m
Option 2: Improved awareness	$0.0m	$0.0m	$0.0m	$0.0m
Option 3: Rules enhancement - central estimate	$57.5m	$0.0m	$0.0m	$57.5m
Option 3 sensitivity	**Business**	**Community organisations**	**Individuals**	**Total**
Low case: 5% incremental uplift	$28.7m	$0.0m	$0.0m	$28.7m

Average annual regulatory costs from business as usual	Business	Community organisations	Individuals	Total
Central case: 10% incremental uplift	$57.5m	$0.0m	$0.0m	$57.5m
High case: 15% incremental uplift	$86.2m	$0.0m	$0.0m	$86.2m

The benefits of Option 3 arise from reducing the expected annual cost of critical infrastructure disruption. This may occur through reducing the likelihood of incidents, reducing the severity or duration of incidents, improving preparedness and response, reducing cascading impacts across interconnected systems, and improving board and government visibility of material risks. These benefits are material but cannot be reliably monetised as a central expected value because the Department does not hold sufficiently robust evidence on the future frequency, severity and timing of avoided incidents or on the marginal effectiveness of each enhancement.

A break-even approach is therefore appropriate with the current evidence base. The preferred option will deliver a net benefit if it reduces expected annual disruption costs by at least the average annual regulatory burden. The reforms do not need to avoid a whole major incident each year to break even. The same result may be achieved by a small reduction in the probability of a high-impact event, a reduction in outage duration or severity, faster recovery, reduced cascading impacts, or avoidance or mitigation of multiple smaller incidents.

Table 5: Break-even implication under the central RBE

2022 RIS disruption scenario	Economy-wide cost	Break-even implication at $57.5m central RBE
Moderate electricity disruption	$850.0m	Avoid one equivalent incident every 14.8 years
Severe electricity disruption	$1.280b	Avoid one equivalent incident every 22.3 years
Severe gas disruption	$1.913b	Avoid one equivalent incident every 33.3 years
Severe water disruption	$4.099b	Avoid one equivalent incident every 71.3 years
Severe liquid fuels disruption	$1.913b	Avoid one equivalent incident every 33.3 years
Severe freight disruption	$724.1m	Avoid one equivalent incident every 12.6 years
Moderate broadcasting/DNS disruption	$3.8m	This scenario alone would not break even; benefits would need to arise from multiple incidents or larger cross-sector impacts

Given the scale of avoided harm associated with disruption to electricity, gas, water, liquid fuels and freight assets, Option 3 would break even if it produces even a small reduction in the expected frequency, duration or severity of high-consequence incidents affecting the in-scope asset classes. The break-even threshold is therefore proportionate to the risk being addressed. Detailed costing, distributional impacts and economic analysis are set out in Section 3.

2.5. Comparative assessment of options

The comparative assessment below summarises the principal advantages and limitations of each option.

Table 6: Comparative assessment of options

Assessment criterion	Option 1: Status quo	Option 2: Improved awareness	Option 3: Enhanced CIRMP requirements
Regulatory change	No change to the CIRMP Rules.	No change to the CIRMP Rules; Government would rely on guidance,	Targeted amendments to the CIRMP Rules for the nine in-scope asset classes only.

Assessment criterion	Option 1: Status quo	Option 2: Improved awareness	Option 3: Enhanced CIRMP requirements
		templates, threat briefings and engagement.	
Effectiveness	Low. Existing baseline obligations would continue, but identified gaps in consistency, maturity and documentation would persist.	Moderate to low. Awareness may improve, but uplift would depend on voluntary uptake and would likely be uneven.	High. Provides clearer, enforceable and auditable requirements for risk areas with inconsistent maturity.
Proportionality	Low in risk terms. Avoids burden but does not respond to the elevated risk profile of the in-scope asset classes.	Moderate. Low regulatory burden, but weaker alignment between risk level and required uplift.	High. Applies only to specified high-risk asset classes and preserves the existing CIRMP architecture, and so far as reasonably practicable principle.
Direct regulatory burden	Nil additional direct regulatory burden.	Nil additional direct regulatory burden, provided measures remain genuinely voluntary.	Central estimate of $57.5 million per year, with a sensitivity range of $28.7 million to $86.2 million per year.
Implementation feasibility	High immediate feasibility, but does not deliver the required uplift.	Moderate. Guidance can be delivered, but implementation depends on entity capability, funding cycles and willingness to invest.	Manageable with staged implementation, guidance, equivalent-framework recognition and flexibility for compensating controls where full technical remediation is not reasonably practicable.
Consultation alignment	Does not respond to stakeholder acknowledgement of the need to strengthen resilience or to intelligence-driven risk concerns.	Responds to stakeholder requests for guidance, but does not respond to feedback that consistent uplift requires clearer regulatory expectations.	Best aligned with consultation when calibrated. Stakeholder feedback has informed extended grace periods, guidance and the principles-based implementation and refinement of prescriptive requirements.
Assessment	Not preferred.	Not preferred.	Preferred option.

2.6. Preferred option

Option 3 is preferred because it delivers targeted uplift within the existing CIRMP architecture, while preserving the so far as reasonably practicable principle and staged implementation.

Option 1 would avoid additional regulatory burden but would not address the widening gap between current baseline CIRMP obligations and the contemporary threat environment. Option 2 would support awareness and voluntary uplift but would not deliver consistent, enforceable or auditable improvements across the in-scope asset classes.

Option 3 delivers targeted uplift while preserving the structure of the existing CIRMP framework. It does not expand the CIRMP to new asset classes and does not apply enhanced obligations to all asset classes subject to the existing CIRMP. It applies only to the nine specified asset classes identified as higher risk. It introduces clearer expectations in areas where consultation and operational experience identified inconsistent maturity:

FOCI, cyber security; including credential compromise and lateral movement, supply chain, personnel security and physical security.

The preferred option is principles-based, incremental and targeted. It maintains the so far as reasonably practicable principle, supports equivalent or compensating controls where appropriate, and is supported by staged implementation periods and guidance. This design responds to stakeholder feedback on implementation feasibility, legacy operational technology environments, supplier concentration, contractor workforces, regulated funding cycles and the need to avoid unnecessary duplication with existing obligations.

The central regulatory burden estimate is materially lower than the original 2022 RIS cost base because the 2026 reforms are incremental to an existing framework, limited to specified asset classes and primarily require additional risk consideration, process uplift, documentation, governance and targeted controls. The preferred option is expected to deliver a net benefit if it reduces annual disruption costs by at least $57.5 million. Given the scale of economic and social harm associated with disruption to electricity, gas, water, liquid fuels and freight assets, this threshold is achievable through even a small reduction in the expected frequency, severity or duration of high-consequence incidents.

There is a residual risk that Option 3 may not go far enough to fully address the pace and complexity of the evolving threat environment, particularly as threat actors continue to adapt and exploit emerging technologies, supply chain dependencies and systemic vulnerabilities. The proposed enhancements are therefore not intended to be exhaustive or static. This risk will be mitigated through ongoing monitoring of the threat environment, continued engagement with the National Intelligence Community and industry, and regular review of the effectiveness of the CIRMP framework.

On balance, Option 3 provides the greatest net benefit because it targets additional obligations to high-risk asset classes, preserves the existing CIRMP architecture, maintains reasonable-practicability principles, and addresses the risk areas where consultation and operational experience indicate inconsistent maturity.

3. Regulatory impact

3.1. Regulatory costing method

The regulatory burden estimate measures the incremental direct regulatory cost of the proposed 2026 enhanced CIRMP Rules relative to business as usual. All responsible entities for the in-scope asset classes are already required to develop, maintain, comply with and annually report on a CIRMP. The 2026 enhancements are therefore costed as an incremental change to the existing CIRMP baseline from the 2022 RIS. This avoids double-counting the costs of activities required under the existing CIRMP Rules, including general risk identification, risk assessment, governance, review, board approval, annual reporting and maintenance of the risk management program.

The Department has adopted a calibrated top-down approach to estimate the incremental regulatory burden of the enhanced CIRMP Rules. Using the 2022 RIS as the reference-class cost base for the existing CIRMP framework and applying bounded incremental uplift factors to the 2022 cost base for the in-scope asset classes. This suggests that the 2026 amendments are a targeted uplift to an established framework, rather than the creation of a new CIRMP regime. The relevant 2022 RIS comparator is the average annual regulatory cost for the asset classes now in scope of the enhanced CIRMP Rules.

The central estimate scenario applies a 10 per cent incremental uplift to that in-scope 2022 RIS cost base. A low case of 5 per cent and a high case of 15 per cent are used to test uncertainty. This range reflects that the enhanced rules are a material but bounded uplift to an existing framework: more than guidance or ordinary business-as-usual, but materially less than establishing the original CIRMP framework. The calculation used is:

Incremental RBE = 2022 in-scope CIRMP average annual cost base × incremental uplift factor.

Table 7: Incremental RBE Scenarios

Scenario	Interpretation	Calculation	Average annual business RBE
Low	Primarily additional risk assessment, documentation, governance, assurance and reporting	$574.5m × 5%	$28.7m
Central	Material but bounded uplift, including some targeted substantive compliance	$574.5m × 10%	$57.5m
High	Higher-burden case with greater substantive uplift in lower-maturity or legacy environments	$574.5m × 15%	$86.2m

The 5 per cent, 10 per cent and 15 per cent assumptions are not presented as a statistical confidence interval. They are transparent sensitivity scenarios designed to test the plausible incremental burden of the enhanced obligations against the best available reference-class cost base.

3.1.1. Treatment of consultation cost information

Consultation submissions provided valuable evidence on cost drivers, implementation constraints and cost-recovery issues. However, the submitted cost estimates are not suitable for direct national extrapolation as the central RBE. Submitted cost estimates were highly variable and often measure-specific, reflecting the circumstances of large entities with complex operational technology environments, regulated funding arrangements, or significant asset portfolios. Some estimates also combined mandatory compliance activities with broader remediation, already planned investments, or implementation choices that may not be required for every responsible entity under a principles-based framework.

The Addendum therefore uses consultation cost evidence to validate the direction and materiality of cost drivers and to inform the high-case sensitivity. The central RBE is instead calibrated to the 2022 RIS cost base for the in-scope asset classes. This provides a more stable and transparent benchmark, avoids over-extrapolating from a non-representative sample, and aligns the costing with the incremental nature of the enhanced CIRMP Rules.

3.1.2. Costing boundary

The central RBE does not assume that every responsible entity will consider every possible technical, cyber, physical, supply chain or personnel remediation activity identified through its risk assessment. The CIRMP framework is risk-based. Its primary regulatory effect is to require responsible entities to identify, assess, document, govern and report material risks, and to minimise or eliminate those risks so far as reasonably practicable.

Accordingly, the RBE includes the incremental cost of mandatory risk consideration, documentation, process development, evidence keeping, governance review, assurance and annual reporting. Substantive compliance costs are included where the rules require a specific capability, process, standard or control, or where such activity is necessary to demonstrate compliance. Costs that reflect business-as-usual activity, voluntary remediation beyond what is required by the rules, indirect pass-through to consumers, direct financial charges payable to government, and enforcement or non-compliance costs are excluded in accordance with the Regulatory Burden Measurement Framework.

Cost layer	Treatment in RBE
Risk consideration and documentation	Included for affected entities where mandatory. This is the core incremental CIRMP burden: assessment, documentation, governance, evidence and attestation.
Process or plan requirements	Included where the rules require processes, systems or plans, including enhanced material-risk and FOCI assessment, supply chain mapping, major supplier assessment, personnel security processes, and physical security and natural hazard processes.

Cost layer	Treatment in RBE
Targeted substantive uplift	Included through the incremental scenario estimate where the rule requires a specific capability or control, such as cyber maturity uplift, MFA, network segregation or background-check administration.
Broader remediation choices	Not automatically included in the central estimate. Included implicitly in the high scenario only, where broader uplift is more likely to be required.
Consumer pass-through	Not included in the RBE because it is an indirect or distributional impact. It is discussed separately.

3.1.3. Break-even analysis

The RBE and break-even analyses serve different purposes. The RBE estimates the average annual direct regulatory burden imposed by the preferred option. The break-even analysis then assesses whether the expected benefits of the preferred option are likely to exceed that burden.

The benefits of the enhanced CIRMP Rules arise from reducing the expected annual cost of critical infrastructure disruption. This may occur through reducing the likelihood of incidents, reducing the severity or duration of incidents, improving preparedness and response, reducing cascading impacts across interconnected systems, and improving board and government visibility of material risks. These benefits are material but cannot be reliably monetised as a central expected value because of the difficulty in predicting future frequency, severity and timing of avoided incidents or the marginal effectiveness of each enhancement.

3.1.4. Small- to medium-sized enterprises and large business impacts

A quantitative split between small- to medium-sized enterprises and large businesses' costs has not been included because the available data does not support a defensible allocation. The current asset-class counts do not identify the responsible entity's size, revenue, workforce or ownership structure. Consultation responses also did not provide a consistent size classification or representative sample that could be used to allocate aggregate burden between small, medium and large entities.

The Addendum acknowledges that cost incidence will not be uniform. Large businesses and regulated network or utility operators are likely to face higher absolute costs because of the scale, geographic dispersion and complexity of their assets. Smaller responsible entities, including some renewable generation, battery storage, DNS or specialised asset operators, may face lower absolute costs but higher proportional burden. This is because several compliance activities have fixed-cost characteristics, including CIRMP documentation, governance review, cyber maturity assessment, supplier due diligence, personnel security processes and audit readiness. Smaller entities may also have less internal cyber, legal, procurement and risk capability, and less bargaining power with original equipment manufacturers, operations and maintenance contractors, and global technology vendors.

This distributional effect is relevant to policy design even though it is not separately quantified in the RBE table. It supports retaining a principles-based approach, staged implementation, guidance, equivalent-framework recognition and flexibility for compensating controls where full technical remediation is not reasonably practicable.

3.1.5. Distributional impacts and consumer pass-through

The proposed enhancements will impose direct compliance costs on responsible entities for the in-scope asset classes. The incidence of those costs will vary across sectors depending on market structure, pricing regulation, cost-recovery mechanisms and competitive conditions.

In economically regulated sectors, such as electricity networks and some water utilities, some efficient compliance costs may ultimately be recovered from customers through regulated pricing or funding processes. This means the reforms may have indirect distributional impacts on households and businesses through electricity, water or wastewater bills. These indirect pass-through impacts are not included in the RBE table because the Regulatory Burden Measurement Framework excludes indirect costs. Still, they are relevant to the overall impact assessment and policy design.

In competitive or trade-exposed markets, cost recovery may be more limited. Liquid fuel operators may have limited ability to pass costs through because pricing is affected by import parity and international competition. Freight operators identified potential competitive neutrality issues in which rail freight providers incur obligations that road freight competitors do not. Smaller energy-transition assets may face higher proportional costs if obligations are applied uniformly, even when they have lower systemic consequences or limited internal capability.

The final policy design mitigates these distributional impacts by limiting enhanced obligations to specified high-risk asset classes, retaining the so far as reasonably practicable principle, allowing equivalent or compensating controls where appropriate, and supporting implementation through guidance and staged compliance periods.

3.1.6. Consultation cost evidence

The matrix at Table 8: Cost Implications of measures by sector from consultation, summarises the incremental cost profile of the enhanced CIRMP measures by sector and obligation category. It reflects the different operating environments, legacy technology constraints, workforce and regulatory settings, and supply-chain exposures identified through consultations. It shows where costs are expected to concentrate, such as cyber maturity uplift and network segregation in OT-heavy sectors, versus areas where the burden is primarily administrative, such as enhanced material-risk assessment and FOCI processes or periodic vendor-of-concern assessments. The matrix should be read by sector (columns) and obligation category (rows), with each cell indicating relative cost impact using the defined severity scale.

Consultation feedback indicated that cyber uplift and system segregation represent the most significant cost drivers, particularly in OT-heavy sectors, driven by legacy environments, supply chain exposure and escalating threat activity. Stakeholders acknowledged that while uplift requires investment, it delivers strong system-wide benefits by reducing the likelihood and impact of major outages, strengthening recovery capability, and aligning practices with widely recognised frameworks such as those listed in the CIRMP Rules. Most stakeholders did not yet provide reliable dollar estimates for these measures, but consistently described them as multi-year, high-complexity uplifts with wide cost dispersion across sectors.

Table 8: Cost Implications of measures by sector from consultation

Hazard Domain	Energy	Water	Transport	Communications
Cyber security framework uplift	**VERY HIGH (!!!)** Strongest concerns across all sectors. OT legacy systems, regulated pricing periods, long outage windows and workforce shortages.	**HIGH (!!)** Legacy OT and constrained regulator pricing periods limit the pace; costs are significant.	**MEDIUM–HIGH (!)** Cost is significant but variable; digital systems are fragmented; the sector asked for proportionality.	MEDIUM (!) Uplift needed, but many entities are already at a higher baseline.
lateral movement	**HIGH (!!)** Operators said three-month isolation was not feasible; segmentation and recovery uplifted significantly across large OT estates.	**HIGH (!!)** Difficult to isolate treatment plants or networks for long periods, need for a recovery-based approach.	**VERY HIGH (!!!)** Three-months of isolation are deemed incompatible with linear networks and safety-critical systems.	MEDIUM (!) Some reliance on cloud- or federated-based identity makes isolation more complex.
Credential compromise	**MEDIUM–HIGH (!)** OT MFA constraints; remote field users; legacy systems.	MEDIUM (!) MFA is workable for IT, but harder on legacy SCADA; request for prioritisation.	MEDIUM (!) Contractor-heavy; MFA constraints for mobile/handheld systems.	MEDIUM (!) MFA constraints for machine-to-machine and DNS operations.

Hazard Domain	Energy	Water	Transport	Communications
Supply chain vulnerability mapping	**HIGH (!!)** Deep global supply chains with single-supplier dependencies.	**MEDIUM–HIGH (!)** Global OEM dependency; mapping is feasible but costly.	MEDIUM (!) Extensive subcontractor chain; mapping possible but resource-intensive.	MEDIUM (!) Suppliers are globally distributed, which maps to a moderate burden.
Supply chain vendor assessment	**HIGH (!!)** Heavy exposure to global vendors; strong need for compensating controls.	MEDIUM (!) Requires clearer thresholds for vendor concern; limited alternatives.	MEDIUM (!) Substitution often difficult; need for Commonwealth guidance.	MEDIUM (!) Concerns that FOCI rules might reduce transparency.
Personnel security plan AND Strengthened background checks	**MEDIUM–HIGH (!)** Very large contractor workforces; regional/remote AusCheck challenges.	MEDIUM (!) Mixed contractor model; AusCheck scalability issues.	**HIGH (!!)** Heavy reliance on contractors; AusCheck is a significant burden.	LOW-MEDIUM (-) Smaller cohorts of critical workers.
Physical security hazards and natural hazards	**MEDIUM–HIGH (!)** Significant costs for perimeter protection, substation hardening, improved access controls and monitoring for widely distributed assets,	MEDIUM (!) Ageing, geographically dispersed plants require upgrades to fencing, access systems, and intrusion detection.	**HIGH (!!)** Open, linear networks make physical security uplift costly and complex.	MEDIUM (!) Need for enhanced site hardening and monitoring of broadcast towers and communications sites.

Severity scale:

- VERY HIGH (!!!): significant cost and feasibility constraints; immediate prioritisation required.
- HIGH (!!): substantial cost or complexity; prioritisation required.
- MEDIUM (!): moderate cost or implementation considerations.
- LOW (-): limited cost or indirect impact.

The costs outlined below at Table 9: Cost Item - Reported Costs per organisation show the range of costs estimated across all submissions received from the in-scope sectors.

Consultation input was inconsistent, and understanding of the proposed rules changes varied, leading to different estimates across submissions. The following table shows the range for which the offered values were substantiated by clear logic. It should also be noted that many submissions declined to provide costs, instead requesting further information on the exact substance of the rule changes.

Table 9: Cost Item - Reported Costs per organisation

Note - Credential compromise hazard and lateral movement hazard, were not consulted on as separate hazard vectors and the costs associated with these measures are reported below are part of the Cyber hazard domain.

Hazard Domain	Upfront Costs	Ongoing Costs (per annum)
All-Hazards	$50,000 - $500,000	$60,000 - $150,000

Hazard Domain	Upfront Costs	Ongoing Costs (per annum)
Cyber	$500,000 - $120,000,000	$100,000 - $4,000,000
Supply Chain	$360,000 - $11,600,000	$50,000 - $2,000,000
Personnel	$25,000 - $1,300,000	$5,000 - $750,000
Physical	$2,000,000 - $3,000,000	$500,000 - $2,000,000

3.2. Economic benefits

Economic benefits arise primarily from avoided or mitigated disruption to critical infrastructure services. The enhanced requirements are expected to improve risk visibility, governance, preparedness, response and recovery across cyber, supply chain, personnel, physical security and natural hazard domains. The benefits are not confined to avoiding major incidents. Benefits may also arise through reduced outage duration, reduced severity, faster recovery, improved escalation to boards, better visibility of dependencies, and reduced cascading impacts across sectors.

Table 10: Economic Benefits

Benefit category	Economic benefit	Mechanism	Impact pathway	Timeframe
System resilience	Reduced frequency and severity of service disruptions	Uplifted cyber, physical, personnel and supply chain controls reduce vulnerability exposure	Fewer outages across energy, water, transport and communications systems support uninterrupted economic activity	Medium to long term
Productivity	Improved operational efficiency within critical infrastructure entities	Standardised and structured risk management processes reduce duplication and reactive responses	Lower operational inefficiencies and reduced downtime improve output across dependent industries	Medium term
Investment confidence	Increased investor and insurer confidence in critical infrastructure sectors	Clear, consistent regulatory expectations reduce uncertainty and risk premiums	Greater capital inflows and more stable insurance pricing support infrastructure investment	Medium to long term
Supply chain stability	Improved visibility and management of critical dependencies	Enhanced supply chain mapping and vendor assessment requirements identify concentration and disruption risks	Reduced cascading failures across interconnected sectors supports the continuity of goods and services	Medium term
Labour market stability	Reduced workforce disruption from insider threats or security incidents	Strengthened personnel security and background checks reduce internal risk events	More stable workforce operations minimise productivity losses and service interruptions	Medium term
Cost avoidance	Avoidance of high-cost incident response and recovery activities	Proactive risk mitigation reduces the likelihood of major incidents requiring emergency response	Lower unplanned expenditure on remediation, legal, reputational and recovery costs	Medium to long term

Benefit category	Economic benefit	Mechanism	Impact pathway	Timeframe
Interoperability	Greater consistency across sectors and jurisdictions	Clarified and formalised requirements create a more uniform baseline of risk management maturity	Easier coordination between operators and Government during incidents reduces systemic impacts	Medium term
Innovation enablement	Safer adoption of emerging technologies	Requirement to assess risks from emerging technologies enables managed innovation	Increased uptake of productivity-enhancing technologies without introducing unmanaged systemic risk	Medium to long term
Asset longevity	Improved protection of physical infrastructure assets	Introduction of physical security planning reduces risks of theft, vandalism and sabotage	Extended asset life and reduced maintenance or replacement costs support long-term capital efficiency	Long term
System-wide risk reduction	Reduced systemic and cascading economic shocks	Holistic, all-hazards risk management improves identification of interdependencies and shared risks	Greater national economic stability through reduced likelihood of multi-sector disruptions	Long term

Overall, the proposed rule enhancements CIRMP supports a more consistent, mature and forward-looking risk management posture across critical infrastructure sectors. This underpins economic stability by reducing systemic vulnerabilities, improving operational efficiency, and enabling sustained investment and growth across the Australian economy. These benefits are consistent with the economic logic applied in the 2022 RIS, which identified avoided disruption costs, improved resilience and continuity of essential services as the primary sources of net economic benefit.

4. Consultation

Consultation on the enhanced CIRMP Rules has occurred in stages. The first stage was a consultation on the proposed enhancements, including policy and impact analysis. Between 9 December 2025 and 13 February 2026, the Department consulted on the Enhancing the CIRMP Rules Consultation Paper. The Exposure Draft consultation document records that the Department received over 60 submissions and engaged more than 1,900 individuals through consultation activities, including two public town halls, two TISN briefings and five TISN impact analysis sessions. The engagement program included 11 online engagements, 1,910 attendees; 7 TISN engagements with 1,652 attendees; 2 public online town halls with 234 attendees; and 2 targeted engagements with utility regulators, with 24 attendees.

Feedback was broadly supportive of strengthening the CIRMP Rules, but consistently emphasised proportionality, reasonable practicability, staged implementation, guidance, alignment with existing frameworks and the practical limits of legacy OT environments, supplier concentration, contractor workforces and regulated funding cycles.

Consultation materially informed the design of the preferred option in this Addendum. In response to feedback, the Department extended grace periods for key obligations, engaged relevant price regulators, committed to developing best-practice guidance alongside the amended rules, retained a principles-based approach, and limited the enhanced requirements to asset classes with an elevated risk profile.

The second stage was consultation on the Exposure Draft of the amended CIRMP Rules from 30 March 2026 to 1 May 2026. The Exposure Draft process invited submissions on the design, implementation, sector impacts and alternative options and sought specific feedback on wording in certain draft provisions. This process enabled stakeholders to provide further comments on the legal implementation of the preferred option before the rules are finalised.

Submissions on the Exposure Draft broadly endorsed stronger requirements for FOCI, cyber maturity, operational technology, supply chain and physical security. There were themes addressing the need to consider proportional application, implementation timing, cost recovery, definitions, offshore and emergency access, supply chain mapping depth, worker impacts, and avoiding duplication with existing regulatory or assurance frameworks.

Table 11: Consultation themes and implications

Theme raised in consultation	Policy design response	Addendum implication
Costs, timeframes and implementation feasibility	Analysis has been prepared; grace periods have been extended; price regulators have been engaged.	Cost uncertainty, regulated pricing cycles and staged implementation.
Asset-class scope and proportionality	Enhanced obligations remain limited to nine specified asset classes identified as higher risk.	RBE and options must remain limited to those asset classes.
Specified risk advice concerns	The original specified-risk-advice workflow is not treated as a standalone final measure; the Exposure Draft reflects enhanced material-risk provisions.	All-hazards 1 has not been costed as a standalone obligation.
Need for guidance and principles-based implementation	Best-practice guidance will be developed; a principles-based CIRMP approach is maintained.	Central RBE does not assume prescriptive capital remediation in all cases.
Cyber uplift, MFA and legacy OT constraints	Exposure draft includes staged implementation and reasonable-practicability language.	Distinguish process/framework uplift from wholesale legacy-system replacement.
Supply chain mapping and major supplier assessment	Framework remains risk-based; government does not propose simple vendor whitelisting or blacklisting.	Include mapping and assessment processes; do not assume supplier replacement as the central case.
Personnel security and AusCheck	Critical worker approach is retained; background-checking and portability issues are subject to co-design and process improvements.	Cost administration and process changes, not checks for all employees.
Physical security plan	Requirement is principles-based and can be integrated with existing arrangements.	Cost plan development and review; capital works only where necessary.

5. Implementation and evaluation

5.1. Implementation

The Enhanced CIRMP Rules provide staged grace periods for the enhanced CIRMP requirements. Sections 6A, 8A(2), and 9A(2), have a 12-month grace period. Sections 8A, other than subsection 8A(2), 8B, 8C, 9A, other than subsection 9A(2), 10A, and 11A, have a 24-month grace period.

This staged approach reflects consultation feedback that responsible entities have different starting points, budget cycles, asset lifecycles, supplier dependencies and operational technology constraints. It also reflects the evolving threat environment. The Department will support implementation through guidance and continued engagement with the TISN and relevant sector forums.

The Department will support implementation through guidance and continued engagement with the TISN and relevant sector forums. Guidance should clarify proportional application and documentation expectations, including equivalent-framework recognition, critical components (including systems) interpretation, compensating controls for legacy environments, supply chain mapping depth, FOCI assessment expectations, critical worker scope and physical security plan content.

5.2. Evaluation

Evaluation of the enhanced CIRMP requirements should occur in two phases: implementation monitoring during the applicable grace periods, and effectiveness assessment after the relevant enhanced requirements have commenced. Success should be assessed by reference to improved clarity, consistency and maturity of risk management practices, rather than incident counts alone.

5.2.1. Implementation monitoring

During the 12-month grace period for material risks, guidance and engagement will focus on how responsible entities intend to consider and address the risks associated with:

- impairments that could prejudice the social or economic stability, national security, or defence of Australia.
- compromise across all hazards as a result of FOCI.
- offshore or remote access to critical components
- offshore or remote access to business critical data
- failure to patch or update operating or security systems in a timely manner
- failure to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued
- deployment or hosting of advanced, novel or emerging technology
- use of advanced, novel or emerging technology against the asset, in a manner that could prejudice the availability, integrity, reliability or confidentiality of the asset
- unauthorised or unsupervised access to critical components
- the compromise or misuse of credentials and privileged access used by individuals to access the CI asset
- access to the CI asset by persons other than critical workers for the CI asset
- incoming and outgoing critical workers.

During the 24-month grace periods, guidance and engagement will focus on whether responsible entities have:

- Incorporated documented cyber framework uplift plans within their CIRMP.
- Implemented phishing resistant MFA to minimise or eliminate credential compromise hazard occurring and mitigate the relevant impact to the CI asset.
- Implemented network segregation to minimise or eliminate lateral movement hazards occurring and mitigate the relevant impact to the CI asset.
- Strengthened background checking and continuous monitoring, including through critical worker mapping and appropriate intelligence background checks for all critical workers.
- Performed vulnerability mapping and vendor assessment, including by clearly identifying affected systems, suppliers, personnel and sites.
- Implemented appropriate security and access plans, including personnel security, physical security and natural hazard plans.
- Demonstrated a credible pathway to compliance by the end of the relevant grace period.

Annual CIRMP reporting and engagement through established regulatory channels will be used to assess whether entities are progressing toward the enhanced requirements. This approach recognises the staged implementation period and supports proportionate regulatory engagement where risks remain elevated.

5.2.2. Effectiveness assessment

Following the attestation period, the evaluation will shift to assessing the effectiveness of the refinements in strengthening risk management maturity and consistency across affected asset classes. Indicators of effectiveness will include:

- Improved consistency and completeness of CIRMP documentation across in-scope asset classes.
- Increased maturity in cyber, supply chain, personnel and physical-security governance.
- Clearer treatment of FOCI, critical systems, critical workers and major suppliers.
- Evidence that entities are using compensating controls and staged implementation, where immediate technical uplift is not reasonably practicable.
- Improved regulator visibility of material risks and planned mitigations.

The evaluation will draw on annual reporting, attestation outcomes, regulatory assurance activities and sector-level trend analysis. The objective is to determine whether the refinements improve clarity, consistency and depth of risk management practice within the existing CIRMP architecture.

Given the dynamic threat environment, findings from ongoing monitoring and post-compliance review will inform future consideration of the CIRMP Rules to ensure they remain proportionate and aligned to national security risks.

Appendix A: Regulatory burden estimate methodology, assumptions and inputs

2022 RIS asset class now in enhanced CIRMP scope	2022 RIS average annual cost ($m)
Critical electricity assets	257.9
Critical gas assets	115.3
Critical water assets	100.7
Critical broadcasting assets and critical domain name systems	1.6
Critical liquid fuels assets	13.2
Critical energy market operator assets	33.0
Critical freight infrastructure and critical freight services assets	52.8
Total in-scope 2022 RIS comparator	**574.5**
Total 2022 RIS all asset classes	**1,150.4**

The 2022 RIS estimated average annual regulatory costs of $1.1504 billion for the full CIRMP framework across all considered asset classes. The asset classes now in scope of the enhanced CIRMP Rules accounted for approximately $574.5 million of that annual average cost. This in-scope comparator is used as the cost base for the 2026 incremental estimate.

The 2026 enhanced CIRMP Rules are not a new risk-management program. They apply to entities already subject to the CIRMP and require incremental uplift in risk consideration, processes, systems, documentation, governance, assurance and targeted controls. The Addendum therefore applies a calibrated incremental uplift to the 2022 in-scope cost base. The low case applies 5 per cent, the central case applies 10 per cent, and the high case applies 15 per cent.

The formula is: average annual business RBE = 2022 in-scope average annual CIRMP cost base x incremental uplift percentage. The central estimate is $574.5 million x 10 per cent = $57.5 million per year. The low case is $574.5 million x 5 per cent = $28.7 million per year. The high case is $574.5 million x 15 per cent = $86.2 million per year.

Sensitivity	Calculation	Average annual RBE	Share of 2022 all-asset-class cost
Low	$574.5m x 5%	$28.7m	2.5%
Central	$574.5m x 10%	$57.5m	5.0%
High	$574.5m x 15%	$86.2m	7.5%

The RBE is not derived from a new bottom-up estimate of hours per activity for each 2026 enhancement. A bottom-up hours model was not adopted because consultation responses did not provide a representative national dataset of marginal time costs, and many submitted estimates combined mandatory compliance activities with broader remediation, already planned investments, or entity-specific implementation choices. The 2022 RIS remains the most complete national activity-based cost base for CIRMP compliance. It incorporated marginal staff effort, labour costs, operating costs and capital costs for the CIRMP framework. This Addendum therefore uses that 2022 in-scope cost base as a reference-class benchmark and applies transparent low,

central and high incremental uplift assumptions to estimate the additional burden of the 2026 enhancements. The table below identifies the incremental activity categories captured by the uplift.

RBE activity category	Treatment in the estimate
Risk assessment and CIRMP updates	Included in the incremental uplift
Governance, assurance and evidence keeping	Included in the incremental uplift
Supplier/vendor review and mapping	Included in the incremental uplift
Cyber maturity assessment, roadmaps and targeted uplift	Included in the incremental uplift
Personnel security planning and critical worker processes	Included in the incremental uplift
Physical security plan development and testing	Included in the incremental uplift
Full remediation of every identified risk	Not assumed in the central estimate
Supplier replacement or major capital works	Not assumed in the central estimate; reflected only in high-side uncertainty where relevant
Consumer pass-through	Excluded from RBE and discussed as a distributional impact

Key assumptions

1. The enhanced CIRMP obligations are incremental to an existing CIRMP baseline.
2. The 2022 RIS remains the most complete national cost base for the CIRMP framework.
3. The relevant comparator is the 2022 cost for the nine asset classes now in scope, not the full 2022 cost across all asset classes.
4. The central estimate reflects a meaningful but bounded uplift in compliance effort.
5. The high case captures entities with lower baseline maturity, legacy OT, constrained supplier markets or more substantive uplift requirements
6. Submitted consultation cost estimates are used for calibration and sensitivity analysis rather than being directly extrapolated, due to non-representative coverage and high variability.

Classification note: The RBE is presented under Business because the 2022 RIS treated responsible-entity costs as business costs, and the affected population is primarily businesses or government business enterprises.

Activities considered

The table below outlines the activities considered for the RBE for the enhanced CIRMP Rules.

Measure	Description	Main incremental RBE activities
Enhanced material risks and FOCI	Responsible entities consider impairment of asset functions and compromise or impairment connected with FOCI.	Risk assessment, supplier/vendor review, CIRMP update, governance and evidence.
Cyber framework uplift	Responsible entities demonstrate Level 2 or equivalent maturity under an accepted framework.	Gap assessment, roadmap, documentation, targeted uplift, assurance.

Measure	Description	Main incremental RBE activities
Credential compromise	Responsible entities implement phishing-resistant MFA where reasonably practicable or manage associated risk through reasonable steps and compensating controls.	Access review, MFA deployment or compensating-control assessment, logging, governance.
Lateral movement	Responsible entities identify critical systems and manage segregation, isolation and recovery planning.	Inventory, architecture review, IT/OT pathway review, recovery planning, documentation.
Supply chain mapping	Responsible entities map major suppliers and critical systems across physical and cyber supply chains.	Supplier identification, data collection, criticality assessment, dependency mapping and evidence.
Vendors of concern	Responsible entities assess and manage vendor risks, including FOCI, concentration, cyber and operational dependency risks.	Vendor-risk process, due diligence, procurement governance and contract review.
Personnel security	Responsible entities maintain personnel security processes, including critical worker identification, access controls, monitoring and background checks.	Role mapping, personnel security plan, onboarding changes, records and AusCheck administration.
Physical security plan	Responsible entities centrally manage physical security and natural hazards and document site, access, monitoring and response measures.	Plan development, site assessment, access-control review, surveillance, alarm review and testing.

Appendix B: Summary of initially proposed enhancements and identified gaps

The proposed CIRMP Enhancements as consulted from 9 December 2025 to 13 February 2026.

Note All-hazard: Specified risk advice did not progress after the first consultation round.

Hazard domain	Current	Identified gap	Enhancement	Nature of change
All-hazard: Specified risk advice	Entities must identify, assess and manage material risks across all hazards in their CIRMP.	Relies on entities' existing review process. No clear requirement for entities to assess specified risk advice or document the response.	Requirement to consider specified risk advice from the Department, assess related material risks, and minimise or eliminate those risks where reasonably practicable.	Clarification and governance uplift within the existing all-hazards framework, not a new hazard domain or prescriptive control.
All-hazard: Material risks – foreign ownership control and influence	Entities are required to consider supply chain and personnel risks in their CIRMP.	No clear requirement for a systematic assessment of FOCI risks across all hazards. Many entities do not apply structured, documented or repeatable FOCI processes.	Requirement to identify and assess FOCI risks, key suppliers and dependencies as part of material risk assessment.	Clarification and structured specification within the existing risk framework.
Cyber: Cyber security framework uplift	Entities are required to maintain baseline maturity (maturity level 1) in their chosen cyber security framework.	Baseline controls are no longer sufficient. Maturity varies widely across sectors. Many entities remain at low maturity.	Uplift in cyber maturity to Maturity Level 2 of suitable cyber security frameworks.	Targeted uplift of cyber maturity expectations.
Cyber: Critical system network protection	Entities must minimise cyber risks to critical IT systems.	No clear standard for logical segregation, isolation or recovery planning for critical systems.	Introduction of clearer expectations regarding IT/OT system segregation, isolation and recovery planning for critical systems.	Specification of control expectations within existing cyber obligations.
Cyber: Multi-factor authentication	General obligation to minimise cyber risks.	Inconsistent use of MFA, particularly for privileged access, remote staff, vendors and machine environments.	Clearer expectations for MFA implementation.	Clarification of control expectation within existing obligation.

Hazard domain	Current	Identified gap	Enhancement	Nature of change
Cyber: Emerging cyber material risks technologies	Obligation to identify and manage material cyber risks.	Existing CIRMP Rules do not explicitly address AI, quantum computing or other advanced, novel, or emerging technology risks.	Requirement to assess and document material risks arising from emerging technologies.	Clarification and extension of material risk consideration.
Supply chain: Supply chain vulnerability mapping	Entities must identify and manage supply chain hazards.	Limited visibility beyond first or second-tier suppliers.	Clearer expectation to identify, map and assess critical supply chain dependencies and vulnerabilities.	Specification of assessment depth and documentation.
Supply chain: Vendors of concern	General obligation to consider supply chain risk.	No clear, consistent process for assessing vendors of concern, including FOCI and concentration risks.	Requirement to establish a documented process for identifying and managing vendors of concern.	Formalisation of governance process within supply chain risk.
Personnel: Personnel security plan	Personnel hazards must be considered within a broader risk management program.	Risks of critical workers accessing sensitive information, including contractors and guests.	Requirement to maintain a documented personnel security plan addressing insider threat and workforce risks.	Formalisation and governance uplift.
Personnel: Strengthened background checks	Entities must manage personnel-related risks.	Inconsistent use of background-checking mechanisms. Uncertainty about critical worker classification and contractor vetting.	Mandating expectations regarding background checks for critical workers and contractors.	Specification of screening expectation.
Personnel: Enhancing personnel material risks	Entities must identify and manage material risks.	Inconsistent identification and documentation of coercion, privileged access misuse and insider risks.	Clearer expectations to identify and document personnel-related material risks.	Clarification of documentation and assessment expectations.
Physical: Physical security hazards and natural hazards	Entities must consider physical and natural hazards in their risk management program.	No requirement to maintain a structured physical security plan comparable to PSPF[11] standards. Inconsistent controls and testing across sites.	Requirement to maintain and test a documented physical security plan.	Formalisation of physical security governance requirements.

[11] https://www.protectivesecurity.gov.au/