INSTITUTE OF STRATEGIC RISK MANAGEMENT

1 May 2026

The Honourable Tony Burke MP
Minister for Home Affairs
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

Dear Minister,

Subject: Feedback on the Exposure Draft of the Critical Infrastructure Risk Management Rules.

Firstly, we would like to thank you for the opportunity to respond to the Exposure Draft of the Critical Infrastructure Risk Management Rules 2026 proposed by the Department of Home Affairs.

The Institute of Strategic Risk Management (ISRM) is a leading global centre for strategic risk and crisis management. Bringing together practitioners, academics, and policymakers from around the world, we foster collaboration, share knowledge and drive innovation in the understanding and application of strategic risk. Through our global network, we support the development of professional capabilities, strengthen resilience and shape the future of risk management.

Our feedback has been drafted by a working group of our Australian fellows and senior members with extensive experience in critical infrastructure (CI) resilience policy, risk management, security and standards development.

We believe that the SOCI legislation should ensure better national preparedness for poly-crisis events; provide better understanding of collaborative CI risk and resilience management responsibilities in supply chain networks; require better proactive measures and versatile decision systems to meet the challenges of current and future, yet undefined, hazards in complex natural and geopolitical environments; enhance and amplify regulatory continuity through alignment with robust adopted international standards; encourage better social engagement and understanding of the criticality of service delivery to communities throughout Australia; develop better adaptive capacities for transforming the way critical services are delivered; and promote even better collaborative learning systems at a national level than those we currently have.

Our detailed comments and recommendations are attached for your further review and consideration
Thank you for your attention

Yours faithfully

[redacted]

[redacted]
ISRM Australia and New Zealand Hub
[redacted]
www.isrm.org.au

ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT

Feedback on the
Exposure Draft of the Critical Infrastructure Risk Management Rules

1 May 2026

Schedule 1 – Amendments Section	Amendment number	Type of comment	Feedback	Proposed change	Further comments and benefits
5 After section 4	4A Application of enhanced CIRMP requirements	general	The current framing emphasises compliance and asset protection, but does not clearly position CIRMPs as part of whole-of-nation preparedness and resilience.	Clarify in the Rules or guidance that CIRMPs support national preparedness by strengthening continuity of essential services, civil resilience, and the ability to sustain critical functions during prolonged disruption.	This would align the CIRMP framework with the national-defence and preparedness logic now emerging in Australian strategic policy.
5 After section 4	4A Application of enhanced CIRMP requirements	general	The Rules do not clearly recognise that resilient critical infrastructure contributes to deterrence by denial by reducing the benefits of coercion, sabotage and grey-zone disruption.	Add interpretive guidance stating that resilience, redundancy and rapid recovery of critical infrastructure are strategic national capabilities, not only regulatory outcomes.	This would connect entity-level risk management with broader national-security objectives and strategic risk reduction.
5 After section 4	4A Application of enhanced CIRMP requirements	general	There is limited visibility of how CIRMP obligations relate to any future national preparedness architecture or wider cross-government resilience arrangements.	Clarify in guidance that CIRMP implementation should, where relevant, align with broader Commonwealth, state and territory preparedness, emergency management and resilience frameworks.	This would reduce fragmentation and help ensure that entity-level planning supports national-level preparedness outcomes.
5 After section 4	4A Application of enhanced CIRMP requirements	general	The Rules do not clearly encourage entities to identify the wider societal and economic consequences of failure of essential functions.	Clarify that CIRMPs should consider not only direct asset impacts, but also downstream consequences for essential services, community stability and economic continuity.	This would reinforce a public-interest and vital-functions approach to critical infrastructure resilience.

ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT

Feedback on the
Exposure Draft of the Critical Infrastructure Risk Management Rules

1 May 2026

Schedule 1 – Amendments Section	Amendment number	Type of comment	Feedback	Proposed change	Further comments and benefits
5 After section 4	4A Application of enhanced CIRMP requirements	general	Governance expectations are not yet framed as a strategic capability in their own right. Recent strategic thinking suggests that governance, assurance and auditability are increasingly "load-bearing" for resilience.	Clarify that boards and senior executives should be able to demonstrate defensible oversight of resilience-critical decisions, including traceability of major risk treatments and assurance of key controls.	This would support stronger accountability and reflect the growing importance of governance as critical infrastructure in itself.
5 After section 4	4A Application of enhanced CIRMP requirements	general	The purpose of CIRMPs is framed primarily around asset protection and compliance. Industry experience indicates that clearer articulation of community and essential service resilience outcomes would support consistent implementation.	Clarify in guidance that CIRMPs support continuity of relevant operators of essential services, community resilience, and necessary activities or controlled goods, in addition to asset protection.	Support for clarification to reinforce resilience outcomes by refining existing obligations, and changes to the CIRMP Rules should be made following ascent of the SOCI Act review.
5 After section 4	4A Application of enhanced CIRMP requirements	general	Senior executive and board oversight expectations are not explicitly articulated.	Introducing more focus on governing bodies declaring the effectiveness of internal controls (similar or aligned with provision 29 of the UK Corporate Governance Code 2024 which came into effect from January 2026).	Support for non-prescriptive clarification to drive consistent governance best practice.
5 After section 4	4A Application of enhanced CIRMP requirements	general	There may be uncertainty regarding the boundary between CIRMP obligations and existing state and territory emergency management responsibilities.	Clarify that CIRMP requirements are intended to complement, not duplicate or contradict relevant frameworks (e.g. NEMA's CASP) and describe how organisational arrangements should align with those frameworks.	Support for clarification to avoid duplication and support coherent multi-level response arrangements.

ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT

Feedback on the
Exposure Draft of the Critical Infrastructure Risk Management Rules

1 May 2026

Schedule 1 – Amendments Section	Amendment number	Type of comment	Feedback	Proposed change	Further comments and benefits
6 After section 6	6A Material risks – enhanced requirements	general	The proposed formulation does not sufficiently capture the reality of a polycrisis environment in which hazards interact, accumulate and reinforce one another.	Clarify that responsible entities should consider concurrent, cascading and sequential disruptions across hazard domains, including scenarios where one hazard weakens the ability to respond to another.	This would improve realism in strategic risk assessment and better reflect the operating environment for critical infrastructure.
6 After section 6	6A Material risks – enhanced requirements	general	Current drafting may encourage static compliance rather than scenario-based strategic risk planning for prolonged disruption.	Encourage responsible entities to use multi-hazard scenario planning and exercising to test continuity of essential functions under sustained and compound stress.	This would support preparedness, not just documentation, and improve decision-making under uncertainty.
6 After section 6	6A Material risks – enhanced requirements	general	The Rules do not sufficiently address the importance of adaptive capacity where entities must operate under constrained personnel, logistics, communications or supplier availability.	Clarify that CIRMPs should consider how essential functions will be maintained under constrained operating conditions, including reduced workforce availability, contested logistics and degraded external support.	Strategic resilience depends not only on prevention, but on the capacity to adapt and continue operating under stress.
6 After section 6	6A Material risks – enhanced requirements	technical	Proposed rule 6A should explicitly require consideration of systemic interdependence, cascading failure, and concurrent disruption across sectors, because the strategic risk environment is increasingly characterised by compounding shocks rather than isolated incidents.	Insert a new provision after 6A(1) requiring responsible entities to consider whether material risks could arise concurrently, cumulatively or sequentially across cyber and information security, personnel, supply chain, physical security and natural hazards, including where disruption in one sector or system may create or amplify disruption in another.	This would better align the Rules with strategic risk management practice, national preparedness, and a polycrisis environment.

ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT

Feedback on the
Exposure Draft of the Critical Infrastructure Risk Management Rules

1 May 2026

Schedule 1 – Amendments Section	Amendment number	Type of comment	Feedback	Proposed change	Further comments and benefits
6 After section 6	6A Material risks – enhanced requirements	technical	The Rules should require responsible entities to consider the role of their asset in supporting national preparedness, civil resilience, defence support requirements, and continuity of essential services during crisis, mobilisation or conflict.	Insert a provision clarifying that, in assessing material risks, responsible entities must consider whether impairment of the asset could affect national preparedness, sovereign industrial capacity, defence support, or continuity of nationally significant services.	This would better align the CIRMP Rules with the 2026 National Defence Strategy and strengthen the strategic purpose of the regime.
6 After section 6	6A Material risks – enhanced requirements	technical	Proposed 2026 Enhanced CIRMP Program rule 6A (a) does not in itself specifically explain or highlight the resilience principles required to plan for unknown risks or surprising impairment of critical infrastructure functions, some of which can realise with very short lead times and serious long term societal consequences. Therefore, we believe specific resilience principles for risk management planning purposes need to be referenced in the Rules to provide the necessary guidance to critical infrastructure entities. Such principles currently exist in a published international standard on infrastructure resilience that is currently scheduled to be adopted as an Australian Standard (AS ISO 22372:2026). It is recommended that the proposed Enhanced CIRMP Rules 2026 be amended to	The first paragraph under Section 6A should be numbered (1). Thus, 6A(a) is renumbered to 6A(1)(a). 6A(b) is renumbered to 6A(1)(b). After 6A (1) (b) a new second paragraph numbered (2) should be inserted with the following intent: "6A (2) For the purposes of paragraph 30AH(1)(c) of the Act, a responsible entity for a CI asset specified in subsection 4A(1) must consider the implementation of the following infrastructure resilience principles in the CIRMP. (a) Principles detailed in AS ISO 22372:2026 Security and resilience – Community resilience – Guidelines for infrastructure resilience"	This would better align the CIRMP Rules with recently published international standards promoting resilient infrastructure, supply chains and communities. It would also provide a common language for understanding and discussing infrastructure resilience and associated risk management planning.

ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT

Feedback on the
Exposure Draft of the Critical Infrastructure Risk Management Rules

1 May 2026

Schedule 1 – Amendments Section	Amendment number	Type of comment	Feedback	Proposed change	Further comments and benefits
			require critical entities to consider those resilience principles. A new sub-section under proposed rule 6A is required to provide this guidance on critical infrastructure resilience improvement in risk management planning.		
6 After section 6	6A Material risks – enhanced requirements	technical	Material risks are expressed predominantly through a security-threat lens. Operational, systemic, environmental, and market risks may be under-considered.	Clarify that material risks include non-malicious risks such as system design limitations, environmental stressors, and market conditions, and common resource pools (CRPs).	Consider this clarification necessary for proportional and adequate risk-based application.
6 After section 6	6A Material risks – enhanced requirements	technical	Control-based risk treatments may be insufficient for high-impact, high-uncertainty events affecting critical infrastructure.	Expand on control layering approaches, and incorporate the definition of "material controls" to include operational, compliance, and narrative reporting, including ESG data.	Consider this clarification necessary for proportional and adequate risk-based application.
6 After section 6	6A Material risks – enhanced requirements	general	The purpose of CIRMPs is framed primarily around asset protection and compliance. Industry experience indicates that clearer articulation of community and essential service resilience outcomes would support consistent implementation.	Clarify in guidance that CIRMPs support continuity of essential services and community resilience, in addition to asset protection.	Support for clarification to reinforce resilience outcomes without expanding regulatory scope.

ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT

Feedback on the
Exposure Draft of the Critical Infrastructure Risk Management Rules

1 May 2026

Schedule 1 – Amendments Section	Amendment number	Type of comment	Feedback	Proposed change	Further comments and benefits
6 After section 6	6A Material risks – enhanced requirements	technical	Material risks are expressed predominantly through a security-threat lens. Operational, systemic, environmental, and market risks may be under-considered.	Clarify that material risks include non-malicious risks such as system design limitations, environmental stressors, and market conditions.	Consider this clarification necessary for proportional and risk-based application.
6 After section 6	6A Material risks – enhanced requirements	technical	Natural disasters are a frequent and foreseeable cause of infrastructure disruption with cascading cross-sector impacts.	Encourage explicit consideration of acute and chronic natural hazard risks, including cascading and long-duration impacts.	Alignment with existing emergency management arrangements should be clarified.
7 After Section 8	8A Cyber and information security hazards	general	The current provisions focus strongly on controls, but less on sustaining operations when controls are degraded or partially bypassed.	Clarify that entities should plan for degraded-but-safe operating modes, including fallback procedures, manual workarounds and prioritisation of essential functions during cyber disruption.	This would make CIRMPs more operationally useful in high-end contingencies and prolonged disruption.
7 After Section 8	8A Cyber and information security hazards	general	Supply-chain mapping alone may not be enough to address strategic dependence on fragile, offshore or contested logistics pathways.	Clarify that responsible entities should assess concentration risk, strategic chokepoints, offshore dependency and restoration feasibility for critical suppliers and enabling services.	This would better capture the strategic dimensions of supply-chain resilience in a deteriorating geostrategic environment.

ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT

Feedback on the
Exposure Draft of the Critical Infrastructure Risk Management Rules

1 May 2026

Schedule 1 – Amendments Section	Amendment number	Type of comment	Feedback	Proposed change	Further comments and benefits
7 After Section 8	8A Cyber and information security hazards	technical	The proposed cyber measures focus on prevention and recovery, but should also more explicitly address degraded operations and sustained disruption where trusted networks, specialist personnel, cloud services or vendor support are partially unavailable.	Clarify in the Rules or guidance that responsible entities should identify and maintain procedures for operating critical systems in a degraded but safe mode for a defined period, including where digital trust is reduced or upstream dependencies are disrupted.	For nationally significant assets, resilience depends on the ability to continue essential functions through disruption, not only to prevent compromise or recover after the event.
7 After Section 8	8A Cyber and information security hazards	technical	Without a clearly defined taxonomic approach of classifying 'domains of criticality' for managed service providers, amended CIRMP rules may unfairly apply to entities by restricting their operational agility and effectiveness under a 'one-size-fits-all' approach.	Clarify the scope of 'managed service providers' delineation between *operators of essential services* and *digital service providers*. Introduce 'criticality' definitions in a tiered approach for both types of entity.	Consider using a services characteristics taxonomy, such as managed services either being: 1. Supplied by an external suppliers 2. B2B vs. B2C 3. Involve regular & ongoing services of data, IT infrastructure & networks, and IT systems 4. Reliance on the providers own network and information system.

ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT

Feedback on the
Exposure Draft of the Critical Infrastructure Risk Management Rules

1 May 2026

Schedule 1 – Amendments Section	Amendment number	Type of comment	Feedback	Proposed change	Further comments and benefits
9 After Section 9	9A Personnel hazards -- enhanced requirements	technical	The personnel provisions focus on suitability, vetting and monitoring, but do not sufficiently address surge workforce resilience and key-person dependency risk in prolonged incidents or national emergencies.	Require responsible entities to identify critical roles whose loss would materially degrade operation or recovery of critical systems, and to maintain succession, redundancy or surge arrangements for those roles.	This would move the Rules from a narrow screening model toward a broader workforce resilience model suited to concurrent crises and sustained disruption.
9 After Section 9	9A Personnel hazards -- enhanced requirements	technical	Responsible Entities of CI Assets increasingly rely on critical workers without Australian Citizenship status to ensure operational capacity under commercial arrangements. By increasing the security clearance requirements of critical workers, administrative pressures will intensify, overwhelm and restrict the processing capacity of AusCheck.	Introduce a co-regulatory arrangement for the SOCI Act, where security vetting agencies certified to the latest version of ISO 28000 - Security and resilience - security management systems) create redundancy for AusCheck processing, and must report to Department of Home Affairs the volume, type and duration of critical worker activities.	Consider a taxonomic approach to the critical worker domains for each CI Asset Class by 'criticality' of the work to be performed.
10 After section 10	10A Supply chain hazards -- enhanced requirements	technical	Supply-chain mapping is necessary but not sufficient. Strategic risk management also requires assessment of concentration risk, sovereign access risk, contested logistics risk, coercive leverage risk and restoration feasibility across critical suppliers and services.	Clarify that responsible entities must consider whether major suppliers, platforms, services or components are subject to concentration, offshore dependency, contested logistics, coercive leverage or restoration-delay risks that could undermine the maintenance or recovery of essential functions during national disruption.	This would better connect CIRMP obligations to national resilience, supply-chain assurance and strategic self-reliance.

ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT

Feedback on the
Exposure Draft of the Critical Infrastructure Risk Management Rules

1 May 2026

Schedule 1 – Amendments Section	Amendment number	Type of comment	Feedback	Proposed change	Further comments and benefits
10 After section 10	10A Supply chain hazards -- enhanced requirements	technical	While major suppliers are undoubtedly important, effective supply chain mapping requires key be identified. Small yet critical suppliers need to be captured.	Change from "major" to "material" suppliers	This would help ensure that small but essential suppliers are not overlooked in the analysis.
10 After section 10	10A Supply chain hazards -- enhanced requirements	technical	Critical infrastructure assets frequently rely on interconnectedness of shared services, networks, resources, and upstream or downstream systems.	Clarify guidance on identification and consideration of compliance warranties for harmonising supply chain 'hardening' requirements i.e. adaptability criteria aligned with key market forces and conditions for each CI Asset Class.	Consider this clarification necessary to strengthen value-level resilience by refining existing regulatory obligations.
10 After section 10	10A Supply chain hazards -- enhanced requirements	technical	Critical infrastructure assets frequently rely on shared services, networks, and upstream or downstream systems. Disruption to one asset or sector may result in cascading or compounding impacts across multiple sectors.	Clarify guidance to encourage identification and consideration of key interdependencies, including shared services and common points of failure, where these may contribute to cascading impacts.	Consider this clarification necessary to support system-level resilience without introducing new regulatory obligations.
11 After 11	11A Physical security hazards and natural hazards -- enhanced requirements	technical	The proposed physical and natural hazard provisions should explicitly address compound hazard scenarios, such as cyber disruption during a natural disaster, telecommunications outage during supply-chain disruption, or insider compromise during emergency response operations.	Add a requirement that responsible entities consider scenarios in which two or more hazards occur simultaneously or in close sequence, including where one hazard reduces the entity's ability to prevent, respond to, or recover from another.	This would improve realism in preparedness planning, exercising and board oversight by recognising the operational reality of a polycrisis environment.

ISRM INSTITUTE OF STRATEGIC RISK MANAGEMENT

Feedback on the
Exposure Draft of the Critical Infrastructure Risk Management Rules

1 May 2026

Schedule 1 – Amendments Section	Amendment number	Type of comment	Feedback	Proposed change	Further comments and benefits
11 After 11	11A Physical security hazards and natural hazards -- enhanced requirements	technical	Natural disasters are a frequent and foreseeable cause of infrastructure disruption with cascading cross-sector impacts.	Clarify guidance on identification and consideration of 'risk event chain reactions', as well as explicitly cover risk response protocols.	Consider alignment with existing emergency management arrangements, as well as international standards (ISO 28000:2022 – Security and resilience - security management systems – requirements, including ISO 28000:2022/Amd 1:2024 Climate action changes).