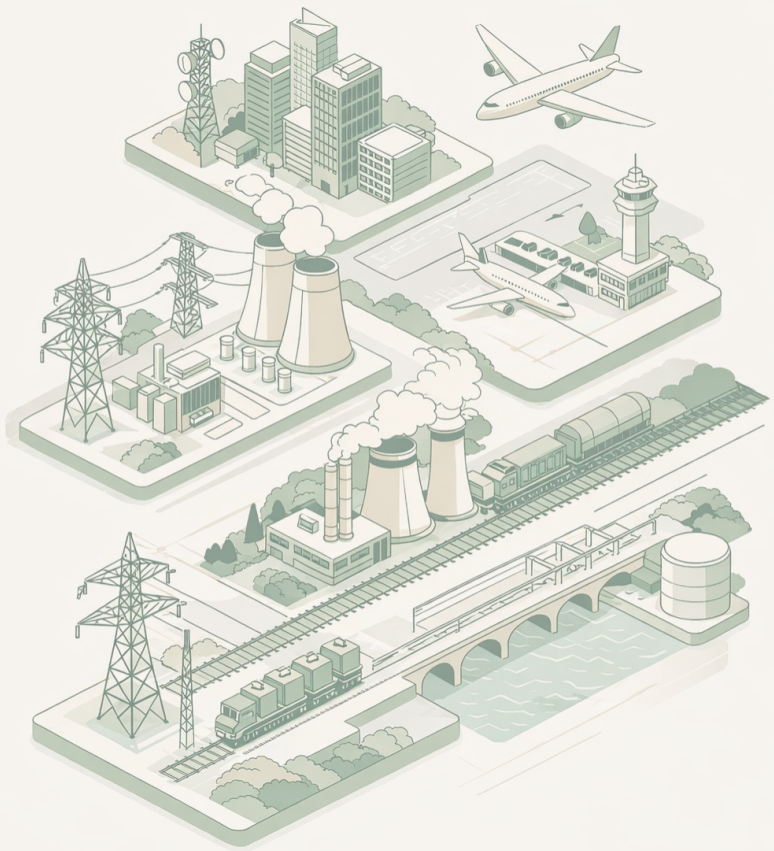
CIRMP Consultation Submission

Elements Information Security Agency



Author

[redacted] | [redacted]

Email

[redacted]

Table of contents

Executive summary

This submission responds to the Department of Home Affairs' (Department) consultation on proposed enhancements to the CIRMP Rules. We support the intent to uplift security posture across high-risk critical infrastructure asset classes in response to documented nation-state threats, particularly the demonstrated Volt Typhoon pre-positioning campaigns and documented vulnerabilities in supply chains. However, we recommend substantial modifications to implementation timelines, regulatory clarity, and cost-benefit proportionality to ensure technically achievable and commercially realistic outcomes.

The enhanced CIRMP measures address documented gaps in Australia's critical infrastructure resilience. The ACSC's Annual Cyber Threat Report 2024-25 demonstrates a 111% increase in attacks targeting critical infrastructure, with 13% of cyber incidents now affecting essential services. ASIO's 2025 Annual Threat Assessment confirms nation-state actors are increasingly mapping and targeting critical infrastructure for strategic pre-positioning. These intelligence assessments justify targeted regulatory uplift for the highest-risk asset classes identified in Table 1 of the consultation paper.

Our principal recommendations are:

1. Support cyber maturity framework uplift to Level 2 with phased implementation but request sector-specific guidance on OT/IT integration challenges for legacy industrial control systems.
2. Support critical systems network segregation requirements but recommend extending implementation timeline to 36 months (June 2029) for brownfield OT environments where air-gapping requires capital-intensive infrastructure redesign.
3. Support supply chain vulnerability mapping with modifications to define reasonable scope boundaries for upstream/downstream tier depth to avoid impractical requirements for complete multi-tier supply chain visibility.
4. Support phishing-resistant MFA requirements with clarifications for operational technology environments where real-time process control systems cannot tolerate authentication latency.
5. Support personnel security plan requirements but request harmonisation with existing industry schemes to reduce duplicative background checking costs.
6. Recommend significant clarification to Foreign Ownership, Control and Influence (FOCI) material risk provisions to define "minimise or eliminate as far as reasonably practicable" where diversification is economically or technically infeasible
7. Recommend procedural safeguards for "specified risk advice" mechanism to ensure consultation on sector applicability and reasonable implementation timeframes.
8. Recommend Physical and Natural hazards to be addressed through models based on international standards such as ISO27001:2022 (physical controls) or frameworks such as ASIO Technical Notes 1/15.

Enhancing the CIRMP Rules

Overview commentary

Executive position

We support the intelligence-driven enhanced CIRMP framework addressing documented nation-state threats through cyber maturity uplift, network segregation, personnel vetting, and supply chain controls creating necessary defense-in-depth. We believe additional modifications are essential for:

1. proportionality via 3-tier criticality classification (nationally critical vs. regionally significant assets) avoiding uniform requirements that over-burden small entities while under-protecting critical ones
2. regulatory coherence through deemed compliance pathways eliminating framework duplication
3. differentiated timelines matching complexity of IT/OT implementation (e.g. 24-30 months for OT architectural changes vs. 6-9 months for MFA) preventing operationally unsafe rushed implementations.

Without these modifications, the CIRMP rules will create compliance-driven operational risks and diverts security investment to duplicative documentation rather than threat reduction.

Recommendations and Rationale

Recommendation	Rationale
R1: Implement NIST-style tiered maturity approach - Adopt 3-tier criticality classification within covered asset classes: - Tier 1 (Nationally Critical): Full enhanced CIRMP measures and expedited timelines (major control centers, critical generation/treatment facilities, nationally significant substations	The current all-or-nothing approach does not differentiate between different-sized operators in sectors. Tiered approaches balance national security imperatives with commercial viability. For example, NIST CSF Tiers demonstrate that graduated maturity models drive continual improvement without overwhelming less-resourced entities. Current uniform

-Tier 2 (Systemically Important): Core enhanced measures with extended implementation windows -Tier 3 (Regionally Significant): Risk-proportionate subset of measures - Classification criteria: interdependency impact (cascade consequences), customer concentration (population served), substitutability (alternative suppliers available), NIC threat targeting assessment	requirements risk under-protection of genuinely critical assets (Tier 1) or over-burdening regionally important but lower-risk assets (Tier 3).
R2: Establish regulatory coherence mechanisms -Create deemed compliance pathways for entities demonstrably meeting equivalent obligations under APRA CPS 230, DISP, or international frameworks (ISO 27001:2023 with Critical Infrastructure supplement). -Develop CIRMP-CPS 230 crosswalk document mapping overlapping requirements (critical operations to critical systems; service provider management to vendor assessment) to enable unified documentation	Regulatory fragmentation imposes opportunity costs - security investment diverted to duplicative compliance activities. For example: Financial Services entities under APRA face duplicative attestation despite conceptual alignment on critical operations and service provider management. APRA-regulated entities already maintain operational resilience frameworks addressing supply chain, cyber, and continuity risks. Deemed compliance reduces burden while preserving security outcomes.
R3: Adopt differentiated implementation timelines -Immediate compliance (6 months): Consideration of specified risk advice, FOCI material risks -Medium-term (12-18 months): MFA, background checking, framework version updates -Extended (24-30 months): Critical system segregation, supply chain mapping, personnel security plans, cyber maturity Level 2 -Mandate quarterly progress attestations with documented implementation plans (as proposed) but extend final deadlines for architectural changes	Implementation complexity varies by orders of magnitude. For example, MFA deployment requires procurement and configuration (6-9 months realistic). Network segregation of OT systems in brownfield environments requires architectural redesign, vendor coordination, safety testing - 18 months is insufficient for responsible execution without operational risk.
R4: Publish asset class selection methodology -Release redacted NIC intelligence assessment summary explaining threat landscape differences between included/excluded sectors -Annual review process for Table 1 expansion/contraction based on updated intelligence (support a PSPF Directions model)	Transparency regarding threat-driven prioritisation builds stakeholder confidence and enables proactive investment. If Defence Industry faces materially higher nation-state targeting yet remains excluded, industry requires clear explanation of DISP vs. CIRMP adequacy assessment.

R5: Introduce proportionality safeguards -Add materiality thresholds (e.g., "where reasonably practicable given asset size, operational complexity, and threat exposure") to measures requiring significant capital investment (network segregation, redundancy systems) -Allow alternative compliance pathways where entities demonstrate equivalent risk reduction through different controls (aligned with ISO 31000 risk treatment optionality)	ISO 31000 emphasises context-specific risk treatment selection. Small regional water utilities face identical requirements as metropolitan operators despite vastly different threat surfaces, budgets, and systemic importance. Proportionality provisions (like NIS2's approach) maintain minimum security baselines while acknowledging operational realities.

All-hazard measures

All-hazard 1: Consideration of specified risk advice

Executive position

We support specified risk advice mechanism with explicit scope boundaries, risk-tiered response timelines (such as 30-day critical/90-day significant/12-month emerging) and mandatory pre-publication industry consultation. This enables government-directed threat intelligence dissemination addressing zero-day vulnerabilities and nation-state campaigns that entities cannot independently identify while ensuring commercial feasibility assessment.

Recommendations and Rationale

Recommendation	Rationale
R1: Establish explicit scope boundaries for "specified risk advice" Define closed list of eligible publication types:	Legal certainty is foundational to principles-based regulation. Unbounded scope creates chilling effect where entities over-invest in tracking every government publication fearing retroactive non-compliance

-PSPF Directions (with sector-specific applicability assessment) -ACSC Critical Alerts and Advisories -Joint FiveEyes threat bulletins affecting Australian infrastructure -ASD Essential Eight uplift notifications for specific threat campaigns. -Exclude generalised guidance documents, TISN discussion papers, or international advisories without Australian contextualisation	findings. For example, CISA's closed BOD taxonomy demonstrates regulatory clarity enables focused compliance investment.
R2: Implement differentiated response timelines based on threat severity -Critical threats (actively exploited, high impact): 30-day implementation requirement -Significant threats (emerging, medium-high impact): 90-day risk assessment + mitigation planning + 12-month implementation -Emerging risks (horizon scanning): 6-month consideration requirement (document risk assessment; implementation only if material risk identified) -Include "reasonably practicable" safe harbor provisions - entities demonstrating genuine technical/commercial barriers receive compliance extensions without penalty	Not all threats are equal. Volt Typhoon actively targeting OT networks demands urgency materially different from horizon-scanning AI risks. CISA BOD 22-01's risk-tiered timelines (15/30 days for exploited CVEs) demonstrate that differentiation balances security imperatives with implementation realism. Uniform 12-month window under-protects against critical threats and over-burdens for low-urgency guidance.
R3: Create structured industry consultation mechanism before advice specification -Minimum 14-day pre-publication consultation with sector TISN groups before designating risk advice as "specified" -Require Regulatory Impact Statement lite for each specified advice publication addressing: -Threat intelligence summary justifying urgency/applicability -Estimated implementation costs and timelines by sector -Alternative mitigation pathways where direct implementation infeasible	PSPF Directions are developed without industry consultation because government is both regulator and regulated entity. Applying them to critical infrastructure private sector requires commercial viability assessment. For example, UK NCSC's collaborative advisory development model shows government-industry co-design produces implementable, effective guidance. Pre-publication consultation prevents unworkable requirements reaching specification stage.

-Possibly expand TISN to include a Specified Risk Advisory Committee (government and industry) to review specification decisions quarterly	
R4: Develop sector-specific threat intelligence dissemination pathways Expand classified information sharing agreements using existing TISN trusted community framework Create sector-tailored specified risk advice rather than blanket PSPF application - energy sector receives OT-contextualized threats; water sector receives SCADA/ICS-specific guidance Mandate Department publication of implementation guidance within 30 days of advice specification, including technical whitepapers, vendor compatibility matrices, and compensating control options	Generic threat advisories create signal-noise problem. Water utility receives energy-sector solar inverter threat despite not operating solar infrastructure - wastes compliance effort. TISN architecture already supports sector channels; leveraging this for tailored intelligence distribution ensures advice relevance and actionability. Classified sharing (used successfully by CISA with critical infrastructure) enables operationally useful threat IOCs.
R5: Shift attestation from process to outcome compliance -Replace "describe consideration process" with: -Risk materiality determination: Entity must attest whether specified risk advice identifies material threat to their asset (Yes/No with justification) -If material: Document implemented controls and residual risk level -If immaterial: Document why threat profile doesn't apply (e.g., "advice addresses cloud infrastructure; entity operates air-gapped OT network") -Reduce documentation burden while increasing accountability for actual risk management	Current proposal mandates documenting "consideration process" – This is an example of compliance theatre that auditors check paperwork rather than security outcomes. Outcome-based attestation (risk materiality and implemented controls) aligns with ISO 31000 risk treatment principles and reduces administrative burden while maintaining accountability.
R6: Establish emergency directive authority with procedural safeguards -Create Critical Infrastructure Emergency Directive power (separate from 12-month specified risk advice) for genuine crises: -Requires Secretary-level authorisation and NIC threat briefing -Maximum 72-hour implementation period for critical actions (e.g., disable	Genuine emergencies exist (WannaCry, SolarWinds, Volt Typhoon pre-positioning) requiring less than 72-hour industry response that 12-month timelines cannot address. An example model: CISA Emergency Directives demonstrate effective urgent authority, but Australian model needs cost-sharing given private sector operators lack government budgets. Procedural safeguards (Secretary authorization,

	compromised software, block malicious IP ranges) -Automatically triggers government cost-sharing mechanism (50% compensation for emergency compliance costs >$100K) -Sunset after 90 days unless converted to formal specified risk advice with standard timelines	90-day sunset) prevent power abuse while enabling rapid threat response.
R7: Integrate with existing ACSC Essential Eight obligations* -Cross-reference specified risk advice with Essential Eight maturity requirements to avoid duplicative obligations -Where advice requires Essential Eight uplift (e.g., patch management for new CVE), consider this satisfied by cyber maturity framework compliance attestation -Prevent entities receiving specified risk advice demanding actions already embedded in maturity level 2 requirements		Proposal creates risk of redundancy with cyber maturity framework uplift. If specified risk advice says "implement MFA" but separate measure mandates MFA via maturity level 2, entities face duplicative attestation. Integration ensures specified risk advice addresses net-new threats beyond baseline framework requirements, reducing regulatory overlap and focusing advice on genuinely emerging risks.

Gaps and Alternatives

1. **Scope and Legal Certainty Issues.** "Non-exhaustive list of possible products" creates unbounded regulatory liability. CIRMP specified risk advice lacks clear delimitation on what constitutes "advisable" versus "mandatory" government publications. PSPF Directions are designed for government entities with different risk tolerances, funding mechanisms, and accountability structures than private critical infrastructure operators. Direct transposition (e.g., DeepSeek ban) creates commercial feasibility challenges - government can mandate immediate software removal; private operators face contract obligations, operational dependencies, and transition costs. This creates interpretive ambiguity in enforcement - does "consideration" require implementation if material risk is identified?
2. [redacted] Suggest that Department aligns specific controls required by Essential Eight ML2 to equivalent ISM controls and/or PSPF controls.
3. **Risk materiality assessment guidance.** Department to publish guidance within 6 months of rule commencement providing risk materiality assessment frameworks for common types of specified risk advice (e.g., software/hardware vulnerabilities, nation-state threat group TTPs, supply chain compromise indicators). Guidance should include decision trees for determining whether specified advice creates material risks for different asset classes.
4. **Frequency limitations.** Establish expectation that specified risk advice will be limited to high-impact, nationally significant threats rather than routine tactical guidance.

Suggest maximum 4-6 specified advice issuances annually to avoid overwhelming entity monitoring capacity

All-hazard 2: All hazard material risks – foreign ownership, control and influence

Executive position

We support FOCI material risk assessment and suggest: operational thresholds with phased 24-month implementation, and compensating control safe harbour framework while acknowledging unavoidable dependencies cannot be unwound in months.

Industry implementation would require government-maintained Vendor Risk Register with classified intelligence integration.

We suggest consolidation of overlapping All-hazard 2/Supply Chain 1/Supply Chain 2 measures into a unified Supply Chain Security Program requirement (eliminates three separate vendor assessments), and mandatory FOCI Risk Assessment Guidance adoption with sector-specific supplements.

Recommendations and Rationale

Recommendation	Rationale
R1: Adopt tiered FOCI definition framework aligned with FOCI Risk Assessment Guidance -Mandate use of three-stage FOCI assessment methodology from Home Affairs guidance: -Stage 1: Establish jurisdictional hazard (classify countries into risk tiers: Low/Medium/High/Critical using NIC intelligence) -Stage 2: Determine exposure (criticality of vendor to asset availability; access to sensitive systems/data; substitutability) -Stage 3: Rate overall FOCI risk (jurisdictional hazard × exposure = risk treatment requirement) -Define control/influence thresholds in Rules or guidance: -Control: >25% voting rights, board appointment rights, golden shares,	Entities may not know what ownership percentage triggers assessment or how to evaluate "influence". Home Affairs FOCI Risk Assessment Guidance already provides operational methodology; mandating its use ensures consistent, intelligence-informed risk evaluation. Jurisdictional tiering (aligned with CFIUS approach) prevents false equivalence between allied and adversary nation vendors.

technology dependencies preventing operation

-Influence: 10-25% ownership, contractual veto rights, sole-source arrangements >AUD $1M annually, access to critical system design/data

R2: Extend implementation timeline with phased compliance approach

Replace 6-month universal deadline with risk-tiered implementation:

Phase 1 (6 months): Identify and assess Tier 1 critical vendors (those whose failure would halt asset operations within 72 hours)

Phase 2 (12 months): Complete FOCI assessment of all major suppliers (top 80% of procurement spend or those with critical system access)

Phase 3 (18 months): Implement risk treatment measures (diversification, compensating controls, enhanced monitoring) for identified FOCI risks

Phase 4 (24 months): Full compliance including lower-tier suppliers and component-level assessment

Mandate documented FOCI Risk Management Plan within CIRMP showing progression through phases with quarterly attestation of progress

Six-month timeline may not be practical in face of supply chain security complexity. For example, the renewable energy sector faces unavoidable Chinese supplier dependencies that took decades to develop – would pose operational disruption in a short timeframe. Phased approach (modeled on IEC 62443 zone/conduit implementation timelines for OT security) may provide better balance of urgency with operational implications, by prioritising critical dependencies while allowing time for comprehensive assessment.

R3: Establish compensating control safe harbour framework for unavoidable FOCI dependencies

-Create four-tier mitigation hierarchy (aligned with CFIUS model):

-Tier 1 (Elimination): Remove FOCI vendor/component (preferred but not always practicable)

-Tier 2 (Containment): Security Control Agreement limiting vendor access to critical systems, data localization, monitoring

-Tier 3 (Enhanced monitoring): Third-party auditing, continuous vendor security assessment, enhanced incident response

"Reasonably practicable" without defined safe harbours could result in identical circumstances judged differently by auditors. The consultation paper acknowledges diversification is often impossible but doesn't specify acceptable alternatives. For example, A CFIUS model of a compensating control framework demonstrates structured mitigation hierarchy enables security outcomes without requiring impossible vendor elimination. Codifying safe harbours could provide regulatory coverage and incentivises investment.

-Tier 4 (Redundancy/resilience): Dual-sourcing where possible, enhanced backup systems, accelerated replacement planning -Entities demonstrating Tier 2-4 implementation for genuinely unavoidable dependencies receive safe harbour from enforcement (deemed "reasonably practicable" mitigation where elimination impossible)	
R4: Develop government-maintained Vendor Risk Register with classified intelligence integration -Establish Critical Infrastructure Vendor Intelligence Service within Home Affairs: -Maintains classified/sensitive register of vendors of concern informed by NIC intelligence (updated quarterly) -Provides confidential vendor risk briefings to cleared responsible entity personnel (CIRMP owners, procurement heads -Issues vendor alert bulletins when new FOCI threats identified (e.g., "Vendor X subject to foreign intelligence law; enhanced controls required")	Private critical infrastructure operators lack intelligence collection capabilities necessary for authoritative FOCI threat assessment. An example, US CFIUS model demonstrates government-led threat intelligence sharing enables effective private sector risk mitigation. Creating Vendor Risk Register leverages existing NIC intelligence that informed measure but isn't accessible to regulated entities and can close the intelligence-action gap. Shifts assessment burden appropriately - government leverages intelligence capabilities; industry implements operational mitigations based on risk determinations
R5: Consolidate FOCI-related measures into integrated Supply Chain Security Framework Merge All-hazard 2, SC1, and SC2 into single Supply Chain Security Program requirement with unified documentation: Component 1: Supply chain mapping (identifying critical dependencies) - from SC1 Component 2: FOCI risk assessment (applying jurisdictional hazard analysis) - from All-hazard 2 + SC2 Component 3: Risk treatment implementation (diversification, compensating controls, monitoring) - integrated approach Create single CIRMP attestation on supply chain security rather than three separate overlapping	Three overlapping vendor assessment measures can be merged into an integrated Supply Chain Security Program provides single coherent framework addressing identification, assessment, and mitigation in logical sequence. Reduces attestation burden (one comprehensive supply chain attestation vs. three partial ones) while improving risk management coherence.

attestations, reducing administrative burden while improving coherence	
R6: Create Mutual Recognition Agreement pathway for entities under equivalent FOCI regimes -Entities subject to CFIUS mitigation agreements, UK NSI Act conditions, or FIRB (Foreign Investment Review Board) FOCI undertakings receive deemed compliance for CIRMP FOCI obligations where: -Existing mitigation measures address same vendor/dependency -Entity provides evidence of compliance with other regime -Department confirms equivalence of mitigation measures	Multi-jurisdictional entities face cascading FOCI reviews - same Chinese vendor assessed under CFIUS (US operations), UK NSI Act (UK subsidiary), FIRB (Australian operations), plus CIRMP. Creates compliance costs without incremental security benefit where regimes substantially equivalent. Mutual recognition reduces duplication while maintaining security outcomes through reliance on allied government oversight.

All-hazard Measures: Regulatory impact analysis

Executive position

All-hazard measure 1: Consideration of specified risk advice.

The measure provides necessary agility to respond to threats faster than traditional legislative amendment cycles permit. However, the 12-month compliance window may prove insufficient for complex operational technology environments where changes require extensive testing, vendor engagement, and planned outage windows. For example, water utilities with distributed SCADA architectures and energy assets with legacy industrial control systems face challenges in rapid implementation of certain risk mitigations.

The mechanism's effectiveness depends heavily on the quality, specificity, and actionability of the risk advice issued. Generic threat advisories without sector-specific implementation guidance create compliance ambiguity and may drive checkbox exercises rather than meaningful risk reduction.

For a representative of our clients, resource requirements: $30K-$80K annually for dedicated threat intelligence monitoring, CIRMP documentation updates, and gap analysis processes. 12 months is achievable for IT-centric mitigations; 18-24 months more realistic for OT environments requiring vendor coordination. For organisations without an existing risk management system (like ISO 27001 or ISO 31001) would require establishing formal processes to monitor Department publications, assess applicability, conduct risk assessments, and document CIRMP updates within attestation cycles.

All-hazard measure 2: All-hazard material risks - foreign ownership, control and influence (FOCI).

This measure appropriately recognises that FOCI risks extend beyond direct ownership to encompass dependencies on foreign-controlled vendors, components, and managed service

providers. However, Australia has unavoidable dependencies on foreign-controlled vendors in some technology domains where domestic alternatives are non-existent or commercially unviable. Elimination may not be practicable, instead mitigation controls can provide acceptable risk management. For a representative of our clients, resource requirements: $100K-$300K for comprehensive FOCI assessments covering ownership structures, vendor relationships, component provenance, and managed service provider contracts. 6 months could be too short for greenfield complex supply chain mapping; 12 months more realistic for thorough assessment and mitigation planning. It requires detailed vendor transparency (often contractually complex), supply chain visibility (limited for multi-tier suppliers), and commercial negotiations for vendor diversification or enhanced controls

For privately owned companies that answer to a Board and/or shareholders, compliance to limit foreign control is unfortunately above the pay-grade of most security professionals. FOCI measures will require additional "teeth" as a foreign majority Board may simply 'accept the risk', with fines being a most cost-effective measure.

Cyber and information security hazard measures

Cyber 1: Cyber security framework uplift

Executive position

We support maturity level 2 requirement with modifications to OT/IT differentiation, timeline flexibility, and equivalence assessment framework. However, the cyber maturity frameworks that are listed are not equivalent, resulting in uneven risk management. [redacted] We suggest instead an equivalent Essential Eight Maturity Level 2 control set of ISM and PSPF controls that are updated in line with revision cadences for both.

International comparison validates level 2 as appropriate baseline. For example, EU NIS2 Directive establishes equivalent "baseline security requirements" for essential entities covering risk management, incident response, supply chain security, and access controls —functional equivalent to structured maturity level 2 capabilities. Although, unlike CIRMP's framework choice flexibility, NIS2 mandates specific technical measures (e.g., encryption, MFA, network segmentation) regardless of framework selection, potentially more prescriptive but with clearer compliance boundaries.

Recommendations and Rationale

Recommendation	Rationale
R1: Differentiate OT and IT maturity requirements with sector-specific timelines -Amend Rules to require: -IT systems: Maturity level 2 within 18 months (June 2028) as proposed -OT/ICS systems: Maturity level 2 within 30 months (December 2028) with mandatory IEC 62443 Security Level assessment for OT components -Hybrid environments (most energy/water assets): Dual-framework approach using C2M2/AESCSF for overall program + IEC 62443 for OT zones, with 30-month timeline for full integration	OT security architectures require extended validation testing to avoid safety system disruption—cannot be implemented on IT timelines. IEC 62443 provides OT-appropriate security level definitions (SL 1-4) addressing ICS-specific threats, while C2M2/AESCSF address enterprise cybersecurity governance. Bifurcated timeline acknowledges operational reality without diluting security outcomes.
R2: Establish formal equivalence assessment framework for non-leveled frameworks -Department publish Cyber Framework Equivalence Guidance specifying: -ISO 27001 equivalence pathway: ISO 27001:2023 certification with Statement of applicability and the annual monitoring audit demonstrating process maturity deemed equivalent to MIL-2 -Essential Eight equivalence: Maturity Level 2 with documented cybersecurity governance framework (policies, roles, metrics) and incident response plan deemed MIL-2 equivalent for IT-focused entities	Current "outline steps taken...to make equivalent" provides no compliance certainty—creates risk of attestation rejection after 18-month implementation. Equivalence guidance provides safe harbor pathway reducing regulatory uncertainty while maintaining security outcomes. Aligns with UK approach where CAF maturity mapping published for common frameworks.

-NIST CSF 2.0 equivalence: Implementation Tier 2 (Risk Informed) across all six functions with documented evidence of repeatable processes deemed MIL-2 equivalent -Self-assessment template enabling entities to map chosen framework controls to C2M2 MIL-2 practices or AESCSF Profile 2 requirements, with auditor validation rather than complete re-assessment	
3: Consolidate overlapping cyber measures into integrated maturity assessment -Eliminate standalone Cyber 2 (network segregation), Cyber 3 (MFA), Cyber 4 (emerging tech risks) as separate requirements—these are control-level specifications redundant with level 2 maturity frameworks: -C2M2 MIL-2 includes: THREAT-2b (network architecture protects critical assets), IAM-2a/2b (authentication and access controls), ASSET-2b (technology lifecycle management) -ISO 27001 includes: A.8.20 (network security), A.8.5 (secure authentication), A.8.6 (capacity management for emerging tech) -NIST CSF 2.0 includes: PR.AC-7 (MFA), PR.DS-5 (network protections), GV.RM-2 (emerging risk management) -Restructure as: Cyber 1: Maturity level 2 requirement (as proposed) with sector-specific guidance on prioritising network segregation, MFA, and emerging technology risks within maturity implementation -Cyber 2-4 measures: Convert to mandatory minimum baselines within level 2 implementation (i.e., entities cannot attest level 2 maturity unless specific controls for network segregation, MFA, emerging tech demonstrably implemented and institutionalised)	Current structure creates artificial distinction between framework maturity and specific controls—entities document network segregation three times (framework compliance attestation, Cyber 2 standalone measure, CIRMP documentation). Precedent for a consolidated approach aligns with NIS2 model where baseline measures (10 minimum requirements) integrate into overall risk management obligation rather than existing as parallel requirements. Reduces documentation burden by ~40% while ensuring critical controls mandated within maturity progression.

R4: Provide phased implementation with capability-based milestones instead of quarterly attestations -Replace "documented plan with quarterly attestation" with phased capability deployment: -Phase 1: Foundation establishment—governance structure, asset inventory, policy framework, role definition (demonstrates organizational commitment and resourcing) -Phase 2: Core security capabilities such as threat management, access controls, incident response processes operationalised (demonstrates repeatable security operations) -Phase 3: Integration and continual improvement with metrics/reporting -OT Phase 4: OT-specific controls validated and integrated with IT program -Attestation at phase completion (3 attestations instead of 7+ quarterly) with objective capability criteria: "Phase 1 complete when governance charter approved, RACI matrix published, asset inventory 80%+ complete"	Quarterly attestations measure planning progress, not security outcomes. Capability-based milestones focus on operationalisation, align with how cybersecurity programs mature, and reduce attestation burden by 60%. This can be seen on C2M2 implementation guidance recommending phased domain prioritisation.
R5: Mandate sector-specific guidance supplements before Rules commencement -Department publish sector-specific maturity implementation guides addressing unique challenges: -Include cost calculators, staffing models, technology procurement guides, and implementation timelines specific to asset characteristics (size, technology stack, geographic distribution)	Generic maturity frameworks fail to address sector-specific contexts—water utility implementing C2M2 MIL-2 has no guidance on whether SCADA telemetry encryption constitutes "network protection" or requires separate control. Sector guidance provides actionable implementation direction, validated technology solutions, and realistic resource planning. An example, NIS2 approach of sector-specific guidance by national authorities demonstrates effectiveness.

R6: Establish maturity progression pathway for entities below baseline -Create accelerated uplift program for entities currently below MIL-1: -Year 1 (by June 2027): Achieve maturity level 1 (initial practices in place -Year 2 (by June 2028): Achieve maturity level 2 (institutionalized practices) -Eligibility: Entities demonstrating current maturity assessment showing <40% MIL-1 achievement -Government-supported implementation assistance: -ACSC/CISC co-development of "Maturity 2 Implementation Playbook" with templates, example policies, control mapping -TISN-facilitated peer learning cohorts enabling small entities to share implementation approaches and technology procurement -Potential co-funding mechanism (similar to UK Cyber Essentials Grant Scheme) for small critical infrastructure operators—AUD $50K implementation grants for entities <100 staff	18-month timeline assumes entities near MIL-1–those substantially below baseline face impossible compliance expectation without transitional pathway. Two-stage progression (1→2) aligns with actual cybersecurity capability development, reduces implementation risk (attempting MIL-2 from MIL-0 produces paper compliance without operational security), and provides government support consistent with consultation paper's acknowledgment that "reforms must be commercially realistic, technically achievable".
R7: Clarify framework version transition requirements and timing -Amend Rules to specify entities currently compliant with previous framework versions (ISO 27001:2013, NIST CSF 1.1, C2M2 v1.1, AESCSF 2020) may: -Option A: Attest continued compliance with previous version through June 2029, then transition to updated version by June 2030 (total 4-year transition period) -Option B: Transition directly to updated version by June 2028 per standard timeline -Gap analysis requirement: Entities choosing Option A must document gap analysis between framework	Requiring simultaneous maturity uplift (ML1 to ML2) and a framework version migration (NIST CSF 1.1 to 2.0 or ISO27001:2015 to ISO27001:2022) within 18 months compounds implementation burden unnecessarily. NIST CSF 2.0 introduces new Govern function with substantial governance structure requirements; ISO 27001:2023 revised controls require documentation updates.

versions and remediation plan by December 2026 -New entities (commencing CIRMP obligation post-Rules commencement): Must comply with updated framework versions only	
R8: Create mutual recognition pathway for entities under equivalent regulatory regimes -Entities subject to APRA CPS 230, DISP, or equivalent international frameworks receive deemed compliance where: -Existing framework requires equivalent or higher maturity (CPS 230 Operational Risk Management effectively requires MIL-2+ capabilities; DISP can mandate ISO 27001 + additional controls) -Entity provides attestation under other regime demonstrating compliance, Department confirms equivalence and scope sufficiency	Financial services entities under CPS 230/234 already implementing robust cyber risk management—requiring separate CIRMP cyber maturity attestation for financial market infrastructure assets creates redundancy. Mutual recognition standard practice in prudential regulation (APRA recognises overseas banking regimes); should extend to cybersecurity frameworks. UK approach recognizes CAF compliance for entities certified to equivalent standards.

Gaps and Alternatives

1. **The cyber maturity frameworks are not like-for-like.** This will result in uneven risk management. From the five frameworks, only ISO27001 is a management system. ISO 27001 is a comprehensive management system with certification (what you must build). Essential 8 is targeted technical controls (what you must do right now) for Microsoft -based systems. NIST CSF is a flexible guidance framework (how to think about cybersecurity). C2M2 is a maturity measurement tool (how mature are you?) Finally, the AESCSF is sector-specific Australian energy framework (C2M2 tailored for Australian energy combining Essential 8 and local requirements). Please see appendix B, Table 2 for further information.
    a. As noted above, the Essential Eight will be superseded by the Foundations of Modern Defensible Architecture. A recommended suggestion is to provide a list of ML2 equivalent controls from both the ISM and PSPF instead, which are updated in line with update cadences from the Department and from ACSC.

Cyber 2: Critical systems network protection

Executive position

Support with mandatory consultation provisions and minimum implementation timeframes. The specified risk advice mechanism addresses the need for dynamic threat response but requires procedural safeguards to prevent unreasonable compliance burdens and ensure sector-specific feasibility assessment.

Recommendations and Rationale

Recommendation	Rationale
R1: Replace uniform 3-month isolation with risk-based isolation tiers which build to 3 month isolated operation -Tier 1 (High-consequence OT - Purdue Level 0-2): 90-day isolation capability (generation control, SCADA field devices, DCS) -Tier 2 (Moderate-consequence OT - Purdue Level 3): 30-day isolation capability (supervisory systems, HMIs, historians) -Tier 3 (Business systems - Purdue Level 4-5): 7-day isolation capability (enterprise applications, reporting, billing)	For entities having to implement from scratch, not feasible. Uniform 3-month requirement ignores operations—core control systems (Purdue 0-2) need extended autonomy, but business systems don't. Risk-based tiers align requirements with consequence of loss. Aligns isolation requirements with asset criticality and operations—core control systems need extended autonomy; business systems have shorter RTOs
R2: Mandate IEC 62443 zone/conduit architecture for OT environments -Amend Rules to require entities with operational technology must implement network segmentation aligned with IEC 62443 zone/conduit principles, achieving Security Level 2 minimum for moderate-risk assets, Security Level 3 for high-consequence assets -Replace "greatest practical level" ambiguity with objective standard -Guidance to include a Zone definition methodology (group assets by function/risk), conduit security requirements (firewall rules, unidirectional gateways), Security Level assessment process	-"Greatest practical" is ambiguous—entities need objective standards meet and the Department to monitor if the CIRMP rules are effective – require a measurable baseline. For example, IEC 62443 provides OT-appropriate segmentation framework addressing industrial protocol constraints that generic IT segregation doesn't capture.

R3: Define "operationally independent" with sector-specific critical functions	Without defining "critical services," entities may over-comply or under-comply. Sector-specific definitions enable realistic planning and clarifies which systems must remain operational vs. which can be suspended, enabling realistic isolation planning.
R4: Specify Recovery Time Objectives (RTOs) and mandate restoration testing -Require documented RTOs for critical system restoration: E.g, Energy (24-72 hours from backup), Water (12-48 hours), Transport (48-96 hours), Communications (4-12 hours) -Mandate annual restoration testing validating rebuild procedures, with test results documented in CIRMP -Require backup architecture documentation: System configuration backups stored offline, restoration runbooks, prerequisite infrastructure (spare hardware, installation media)	"Plan to rebuild" without validated procedures creates false confidence—annual testing ensures restoration capability exists when needed.
R5: Consolidate network segregation into Cyber 1 maturity requirement -Eliminate Cyber 2 as standalone measure—integrate as mandatory baseline within Cyber 1 maturity level 2 attestation -Entities cannot attest MIL-2 compliance unless network segregation demonstrably implemented per ML2 equivalent framework	Level 2 frameworks already mandate network protections — separate requirement creates artificial distinction without security benefit Single attestation covering maturity**,** segregation and isolation capability reduces documentation burden.
R6: Extend implementation timeline to 30 months for OT network redesign -IT system segregation: 18 months (June 2028) -OT network architecture (zone/conduit implementation): 30 months (December 2028) -Phased milestones: 12 months (asset inventory and zone definition), 24 months (conduit design and procurement), 30 months (staged rollout and validation)	OT network redesign requires 24-36 months for safety validation, staged testing, regulatory approvals. 18-month timeline risks rushed implementations compromising operational safety. Cannot redesign operational SCADA architecture on IT timelines—safety system validation, staged testing,

	regulatory approvals require extended periods
R7: Provide government-supported zone/conduit implementation guidance -ACSC and/or Department publish sector-specific zone/conduit reference architectures: -Include: Sample zone definitions, conduit security requirements, firewall rule templates, unidirectional gateway specifications, restoration architecture examples -Cost modeling: Typical implementation costs by facility size/complexity with ROI analysis showing lateral movement risk reduction -Vendor guidance: OT-compatible firewall solutions, IEC 62443-certified products, air-gap data diode - technologies	Generic "implement segregation" without implementation roadmap produces inconsistent outcomes—sector guidance provides clear direction.
R8: Establish realistic isolation testing requirement -Require annual 7-day isolation exercise (not full 90 days) validating critical systems operate without external connectivity -Document: Systems tested, connectivity removed, functionality validated, issues identified, remediation actions -Progressive testing approach: Year 1 (24-hour isolation), Year 2 (7-day isolation), Year 3+ (maintain 7-day capability, test annually)	3 month isolation testing operationally impractical (requires extended outage windows, customer notification, regulatory approval)—7-day testing validates architecture without excessive disruption while building confidence in capabilities
R9: Address air-gap bridging technologies for operational requirements -Acknowledge legitimate needs for OT data extraction (remote monitoring, predictive maintenance, cybersecurity visibility) while maintaining isolation capability -Mandate unidirectional gateways/data diodes for OT-to-IT data flows where real-time monitoring required	"3-month isolation" conflicts with operational needs for remote monitoring—unidirectional architectures enable data visibility while preventing reverse compromise

-Prohibit bi-directional remote access to Purdue Level 0-2 systems; require jump servers with MFA for Level 3 supervisory access -Document all air-gap bridging points in CIRMP with compensating controls (authentication, logging, access restrictions)	
R10: Clarify interaction with existing cyber monitoring obligations -Require: Internal OT monitoring capabilities within isolated environment (local logging, anomaly detection, insider threat monitoring independent of enterprise SOC)	How do isolated systems maintain mandatory cyber incident detection? If SIEM/EDR disconnected during isolation, entity blind to compromise. Consider portable incident response capabilities—USB-based forensics tools, air-gap jump kits, local analysis workstations for use during extended isolation Isolation protects against external threats but must maintain visibility into insider threats, misconfigurations, equipment failures occurring within isolated environment

Gaps and Alternatives

1. **Unclear rationale** that "critical systems are operationally independent...such that they can be isolated for a period of 3 months while maintaining critical services" appears derived from ASD CI Fortify guidance but lacks sector-specific rationale.
2. **No Guidance on "Operationally Independent" Definition.** What systems must remain operational during 3-month isolation? Core control functions only? Business operations (billing, HR)? Customer interfaces? Case study (payroll system isolation) uses low-risk example—doesn't address high-consequence interdependencies like SCADA historian data, remote diagnostics, cybersecurity monitoring tools
    a. E.g. Energy: Can grid operate without market data feeds? Water: Can treatment continue without lab results uploaded to LIMS? Transport: Can freight tracking function without GPS connectivity?
    b. Define "critical services" operationally per sector—energy maintains generation/transmission/distribution; water maintains treatment/pumping; transport maintains physical movement (excluding ancillary business functions)

Cyber 3: Multi-factor authentication (MFA)

Executive position

We support phishing-resistant MFA for materially reducing credential compromise.

We suggest compensating controls for OT/SCADA environments where air-gapped networks, safety-certified configurations, and legacy HMI systems lack MFA support. To support roll-out of phishing resistant MFA we suggest a phased implementation prioritising privileged/critical system users.

We suggest including mandatory break-glass emergency access procedural requirements to ensure security controls don't compromise safety during genuine operational emergencies.

Recommendations and Rationale

Recommendation	Rationale
R1: Establish compensating control framework for MFA-incompatible systems -Formally define acceptable alternatives where phishing-resistant MFA "not reasonably practicable": -Tier 1 (Preferred): Jump server/bastion host with phishing-resistant MFA protecting access to non-MFA legacy system and session recording -Tier 2 (Acceptable): Local console access only, physical security controls (locked control room, access card logs, video surveillance), no remote access permitted -Tier 3 (Temporary): Enhanced behavioral analytics, strict IP whitelisting, time-limited access windows, mandatory dual-person authorization for privileged actions -Tier 4 (Legacy transition): Traditional MFA (OTP) and compensating controls during 24-month migration to phishing-resistant methods -Require documentation in CIRMP suggest including systems using compensating controls, justification, mitigation timeline (max 24 months for Tier 3/4)	Legacy OT systems cannot support MFA without costly recertification; measure asks about impracticality but provides no guidance. Compensating controls (jump servers, physical security, behavioral analytics) maintain security during transition.

R2: Provide phased implementation timeline based on user risk tiers -Phase 1 (12 months): Privileged users, critical system administrators, remote access (typically 15-25% of workforce) -Phase 2 (24 months): Users with access to sensitive data, business-critical applications (next 50-60%) -Phase 3 (36 months): All users accessing organizational systems (remaining 15-35%)	Progressive deployment reduces costs (spread hardware token procurement over 3 years), enables lessons learned from early phases, prioritizes highest-risk access Aligns with Essential Eight maturity progression, ML1 covers internet-facing services and ML2 expands to all systems
R3: Mandate break-glass / emergency access procedures -Require documented emergency access procedures in CIRMP. Examples include: -Break-glass codes: Time-limited bypass credentials stored in sealed envelopes, tamper-evident physical security, authorized by two supervisors -Backup authentication methods: Secondary FIDO2 keys stored in secure location, supervisor-issued temporary tokens -Emergency activation process: Clear escalation path, documented approval authority, automatic expiration (4-24 hours depending on criticality) -Post-incident requirements: All emergency access logged, reviewed within 24 hours, incident report documenting justification and actions taken	Critical infrastructure 24/7 operations cannot tolerate authentication failures preventing emergency response—break-glass ensures security doesn't compromise safety

Cyber 4: Enhancing cyber material risks

Executive position

We support with clearer parameters for emerging technology assessment and integration with existing risk management processes. The current threat landscape requires adaptive risk identification beyond static framework compliance. This measure appropriately recognises that prescriptive controls cannot address all emerging threats.

However, the measure's scope requires clarification. "Novel technologies on the horizon" encompasses an extremely broad range of potential developments. Without parameters, this could create compliance ambiguity and inconsistent interpretation across entities and auditors.

What is being asked of industry is to conduct a risk assessment and risk treatment against what the Department is calling cyber material risks and suggest that the Department provide the risks and a mechanism of reporting risk assessment results (i.e. low medium high) on the entity, including a summary of the risk treatment plan for each risk to the Department.

Cyber and information security hazard: Regulatory impact analysis

Executive position

Cyber measure 1: Cyber security framework uplift (ML2).

Uplift from maturity level 1 to level 2 is justified given the sophistication of state-sponsored threats like Volt Typhoon, Salt Typhoon, and APT29. Current baseline protections have proven inadequate against advanced persistent threats employing living-off-the-land techniques and patient lateral movement strategies.

For a representative of our clients, resource requirements: $200K-$800K depending on current maturity (gap analysis, control implementation, technology acquisition, staff training, audit/attestation costs). 18 months achievable for mature IT environments; 24-30 months more realistic for OT-heavy assets requiring industrial control system upgrades. OT environments face vendor dependencies for security patches, limited MFA capabilities in legacy SCADA systems, and operational safety implications requiring extensive testing

Cyber measure 2: Critical systems network protection

The requirement to maintain critical services during 3-month isolation periods reflects realistic threat scenarios where incident response and remediation require extended timeframes. However, this requirement may be operationally impractical for assets with interdependencies on enterprise systems (e.g., SCADA systems requiring corporate network connectivity for vendor remote support, regulatory reporting, or business intelligence).

The system rebuild capability requirement is sound security practice but requires significant investment in backup infrastructure, documented rebuild procedures, and regular testing—capabilities currently absent in many operational technology environments. For a representative of our clients, resource requirements: $300K-$1.2M per site for network architecture redesign, segmentation infrastructure (firewalls, jump hosts, data diodes), backup systems, and rebuild testing. 30-36 months realistic for comprehensive OT network segmentation projects requiring design, procurement, testing, and staged implementation.

Cyber measure 3: (Phishing resistant) Multi-factor authentication (MFA).

The measure appropriately extends MFA requirements beyond those specified in some maturity level 2 frameworks, creating a consistent baseline across all high-risk assets. Centralised logging of authentication attempts enables detection of credential stuffing, brute force attacks, and compromised account activity.

However, many legacy OT systems (SCADA HMIs, engineering workstations, industrial controllers) lack native MFA capabilities. Retrofitting requires gateway solutions, protocol translators, or system replacements—investments with extended procurement and implementation timelines. Additionally, some emergency access scenarios (e.g., physical console access during network failures) may require documented exception processes. For a representative of our clients, resource requirements: $50K-$250K per site for OT-compatible MFA solutions, gateway infrastructure, privileged access management systems, and authentication logging infrastructure. 12 months achievable for IT systems; 24-30 months realistic for OT environments requiring vendor engagement and legacy system solutions. Legacy SCADA/DCS systems often lack native MFA support; some industrial protocols incompatible with modern authentication methods; emergency access procedures will also require careful design.

Cyber measure 4: Enhancing cyber material risks

What is being asked of industry is to conduct a risk assessment and risk treatment against what the Department is calling cyber material risks and suggest that the Department provide the risks and a mechanism of reporting risk assessment results (i.e. low medium high) on the entity, including a summary of the risk treatment plan for each risk to the Department. For organisations without a risk management system (i.e. ISO27001, ISO31001)

. For a representative of our clients, resource requirements $40K-$100K annually for threat intelligence subscriptions, emerging technology assessments, and CIRMP documentation updates. Costs are higher if a risk manager (or equivalent like information security manager, GRC Manager) is required i.e. 2 FTE $180-$200K per FTE. For greenfield implementation – 12 - 18 months depending on organization size and maturity. An ongoing obligation with 6-month assessment cycle reasonable

Supply chain hazard measures

Supply Chain 1: Supply chain vulnerability mapping

Executive position

We support integrating a process or system for supply chain vulnerability mapping. We think it requires objective multi-tier scope definition, major supplier criteria, vulnerability assessment methodology, and consolidation of Supply Chain 1/Supply Chain 2/All-hazard 2 into unified Supply Chain and Vendor Risk.

We suggest a tiered diversification framework recognising implementation in practice and linking supply chain measures to business continuity measures.

Recommendations and Rationale

Recommendation	Rationale
R1: Define structured supply chain mapping scope requirements -For example: -Upstream mapping: -Tier 1 (direct suppliers): All suppliers >$100K annual spend OR providing critical systems/services OR having remote access to entity networks—100% mapping required -Tier 2 (sub-suppliers): Critical components with <3 alternative global suppliers OR intelligence-identified high-risk jurisdictions—targeted mapping	A structured scope (Tier 1 comprehensive, Tier 2 targeted critical, Tier 3 intelligence-driven) provides a realistic boundary for supply chain mapping. Map supply chain for major suppliers is not clear on the depth required i.e. Tier 1 only is insufficient to identify Tier 2-3 risks like solar inverter vulnerability cited in consultation.

-Tier 3: Only where government specifies sector-specific concern (e.g., solar inverter manufacturers, telecommunications equipment)

-Downstream mapping: Distribution partners with access to critical infrastructure data OR managed service provider customers where entity provides critical services

-Minimum data fields: Supplier name, jurisdiction, ownership structure, criticality rating, replaceability assessment, remote access status, alternative suppliers identified

R2: Clarify "major supplier" with objective criteria

-For example, major supplier defined as meeting ANY of:

-Revenue >$500K annually OR >5% of procurement category spend

-Supplies critical components/services with <3 qualified alternative suppliers globally

-Provides services essential to asset availability (OT maintenance, SCADA support, cybersecurity monitoring, emergency response)

-Has network/remote access to entity IT or OT systems

-Identified in intelligence assessments as posing sector-specific risk (e.g., energy sector DER equipment suppliers)

"Major supplier" undefined creates compliance ambiguity—$10M IT contract vs. $500K sole-source SCADA component, which is major? Objective criteria (spend OR criticality OR access OR <3 alternatives) ensures high-risk low-spend suppliers captured, aligns with risk-based approach.

R3: Require separate physical and cyber supply chain mapping

-Physical supply chain map: Manufacturing (component sources, Tier 1-2), logistics (transport, warehousing), spare parts providers, consumables, field service contractors

-Cyber supply chain map: Software vendors (OT applications, enterprise software), SaaS platforms, MSPs/MSSPs, cloud providers, cybersecurity tools, vendors with remote access privileges, software update/patch sources

-Integration point: Identify suppliers appearing in both (e.g., OT vendor providing both hardware and remote

"Physical and cyber supply chains" distinction unclear as entities may map physical manufacturers but miss software vendors, MSPs with remote access.

Separate mapping requirements ensure comprehensive coverage. An example framework is NIST 800-161 hardware/software/service supply chain framework.

monitoring software)—highest risk category requiring enhanced controls	
R4: Mandate a structured vulnerability assessment methodology -This assessment methodology might require: -Documented assessment of each major supplier across four dimensions: -Criticality (1-5 scale): Operational impact if supplier lost/compromised—5=immediate asset unavailability, 1=minor inconvenience -Replaceability (time in months): 1=<1 month alternative available, 5=>12 months or no alternative exists -Security posture: FOCI risk (foreign ownership/control), cyber maturity (ISO 27001/equivalent), financial stability (credit rating), incident response capability -Concentration risk: Geographic (>50% suppliers same region), vendor (>30% spend single vendor), single point of failure (sole-source for critical function)	"Identify critical vulnerabilities" is unclear in practice with no guidance on how to assess vulnerability in this context. A uniform vulnerability methodology will provide a baseline for both industry and the Department. An example: NIST 800-161 structured approach (criticality × replaceability × security × concentration) can give uniform data.
R5: Establish tiered diversification requirements based on criticality -Tier 1 (High-criticality, easily replaceable): Mandatory ≥2 qualified suppliers, procurement split to maintain both relationships, 90-day alternative supplier activation capability -Tier 2 (High-criticality, difficult to replace): Sole-source acceptable with: 6-12 month inventory buffer for critical components, documented alternative supplier development plan (timeline to qualify new source), enhanced monitoring of sole-source supplier financial/operational health -Tier 3 (Medium-criticality or replaceable): Single-source acceptable with documented alternative controls: supply chain monitoring, expedited procurement procedures, mutual aid agreements with other entities -Tier 4 (Low-criticality): No diversification requirement, standard procurement practices sufficient	"Where possible...supplier diversification" provides no meaningful requirement since entities can claim diversification "not possible" without justification. Tiered approach recognises legitimate sole-source scenarios (i.e. renewable energy equipment) while requiring enhanced controls (inventory buffers, development plans) where diversification is impossible. Recognises that some diversification impossible while ensuring high-risk dependencies have mitigation.

R6: Create integrated "Supply Chain and Vendor Risk Register"

-Single consolidated register satisfying Supply Chain 1 (mapping), Supply Chain 2 (vendors of concern), All-hazard 2 (FOCI) requirements simultaneously

-Required fields per supplier:

-Basic information (name, jurisdiction, ownership, products/services provided, annual spend)

-Criticality assessment (SC1 vulnerability scoring)

-FOCI assessment (All-hazard 2 foreign control/influence analysis)

-Vendor of concern determination (SC2 risk rating and compensating controls)

-Alternative suppliers identified, diversification status, contingency plansAligns with NIST CSF 2.0 unified third-party risk management approach

SC1, SC2, All-hazard 2 may assess same suppliers with overlapping criteria an integrated register with single assessment process would increase compliance and streamline data handling for the Department.

R7: Mandate supply chain mapping integration with business continuity plans

-Require documented "Supply Chain Continuity Playbooks" for each Tier 1-2 critical vulnerability covering:

-Alternative supplier activation: Pre-qualified alternates, procurement lead times, technical qualification requirements, contractual frameworks

-Inventory surge capacity: Critical component buffer stocks (3-12 months depending on replaceability), storage locations, refresh schedules

-Supplier compromise response: Procedures if supplier experiences cyber incident, financial distress, geopolitical disruption, natural disaster

-Annual testing: Tabletop exercises simulating supplier loss, alternate activation drills, continuity plan updates based on lessons learned

Supply chain map without business continuity integration becomes static compliance document.

An example model - ISO 28000 requires continuity planning with incident response, alternative activation procedures, regular testing. Playbooks transform mapping into actionable risk management, which supports Cyber 2 restoration requirements.

R8: Require Tier 1 critical supplier security assessments

-Mandate Security Assessment Questionnaire (SAQ) for all Tier 1 major suppliers annually covering:

-Cyber maturity: Own CIRMP/ISO 27001/equivalent compliance, incident response capability, cyber insurance coverage

-Access controls: If remote access provided, MFA implementation, session monitoring, access logging, jump server architecture

-FOCI structure: Ownership disclosure, foreign control/influence assessment (cross-reference All-hazard 2), government relationships

-Financial stability: Credit rating, recent financial performance, dependency on entity (% of supplier revenue), business continuity plan existence

-Incident notification: Contractual requirement to notify entity within 24 hours of cyber incident, supply disruption, ownership change

-For non-responsive suppliers or adverse assessments, require enhanced monitoring or alternative supplier development

Mapping identifies suppliers but not their security posture. E.g. SolarWinds incidents demonstrate trusted supplier with weak security becomes attack vector.

Model frameworks E.g.NIST 800-53, CSF 2.0, ISO27001 require ongoing supplier security assessments. SAQs validate supplier cyber maturity, enable risk-based decisions (maintain/enhance/replace).

R9: Provide government supply chain mapping guidance and tools

-Sector-specific mapping templates (energy, water, transport, communications) pre-populated with common supplier categories

-Approved supply chain risk management (SCRM) platform list—software options, capabilities, typical costs ($10K-$100K), implementation best practices

-Supplier security assessment questionnaire (SAQ) template aligned with CIRMP requirements

-Cost modeling: Small entities $20K-$50K (consultant-assisted mapping, spreadsheet-based), medium $50K-$150K (SCRM platform implementation), large $150K-$400K (enterprise SCRM platform, automated monitoring)

Complex supply chains (1,000+ suppliers) require software tools—spreadsheets insufficient for effective mapping.

Government guidance on SCRM platforms, methodologies, sector templates reduces implementation uncertainty, prevents duplicative tool procurement, enables consistent approach across sectors.

Supply Chain 2: Vendors of concern

Executive position

We support the vendor of concern assessment measure but require objective "vendor of concern" definition, mandatory FOCI Risk Assessment Guidance, tiered compensating controls framework and suggest consolidation with Supply Chain 1/All-hazard 2 into unified Supply Chain Risk Register.

We suggest government-operated classified TISN Vendor Threat Briefing program and "no practical alternative" determination methodology to prevent undefined "vendor of concern" creating compliance ambiguity. We suggest compensating controls acceptable for unavoidable high-risk sole-source vendors, and controls on potential sole-source loophole claims that could enable non-compliance.

Recommendations and Rationale

Recommendation	Rationale
R1: Define "vendor of concern" with objective criteria -E.g. Vendor of concern = meets ANY: FOCI risk assessment score ≥15 (high risk per government guidance), operates from intelligence-specified jurisdictions/entities (published via TISN), failed security assessment (SAQ score <60%), subject to coercive foreign laws (National Security Law, State Secrets Law equivalents)	"Vendor of concern" undefined creates compliance ambiguity. Objective criteria (FOCI score threshold, intelligence-specified, security failure, coercive laws) provides clear, actionable definition enabling consistent application across 300+ entities.
R2: Consolidate SC1, SC2, All-hazard 2 into unified supply chain risk register	Repeated recommendation from Supply Chain 1.
R3: Mandate compliance with FOCI Risk Assessment Guidance methodology -Suggest replacing "consider principles" with "implement methodology per FOCI Risk Assessment Guidance or equivalent ISO/NIST third-party risk framework "	"Consider principles" weaker than compliance mandate–enables inconsistent application. FOCI Risk Assessment Guidance provides structured flow of, repeatable assessments: Stage 1 vendor review questionnaire; Stage 2 FOCI risk assessment (3 steps: identify, assess, recommend); Stage 3 implement mitigations

R4: Require vendor risk scoring and tiering system -An example: Composite risk score: Supplier criticality (1-5, from SC1) × FOCI exposure (1-5, ownership/jurisdiction/control) × Security posture (1-5, from SAQ) = score 1-125. -Tiering: High risk (≥60), medium (30-59), low (<30)	No risk scoring prevents resource prioritiation—$500K available, mitigate Vendor A or B? Composite scoring (criticality × FOCI × security) with tiering (high/medium/low) enables proportional resource allocation per best practice vendor risk management.
R5: Define tiered compensating controls framework -High-risk vendors (score ≥60): Network isolation (air-gap from critical systems per Cyber 2), offshore access prohibited (exceptions require Secretary approval), continuous monitoring (weekly vulnerability scans, monthly audits), contractual audit rights, 12-month alternative supplier development plan -Medium-risk (30-59): Standard cyber hygiene (MFA, logging, quarterly reviews), restricted access (not to critical systems), alternative supplier identified -Low-risk (<30): Annual reassessment only	"Additional security measures" unspecified. What controls are acceptable for high-risk sole-source vendors? A tiered framework based on FOCI Guidance mitigation hierarchy and compensating control frameworks provides clear implementation guidance.
R6: Mandate ongoing vendor monitoring and reassessment -Annual reassessment: High-risk vendors -Biennial: Medium-risk vendors -Triggered reassessment (within 30 days): Ownership change (acquisition, merger), security incident (breach, compromise), intelligence notification (government identifies new risk), jurisdiction change (operations relocated) -Continuous monitoring for high-risk: threat intelligence feeds, dark web monitoring, financial stability tracking	One-time assessment is inadequate vendor risk dynamic (ownership changes, security degradation, intelligence updates). Ongoing monitoring (annual for high-risk, triggered for material changes) + continuous threat intelligence for highest-risk ensures currency per third-party risk lifecycle management.
R7: Provide classified TISN Vendor Threat Briefing -Quarterly classified briefings (SECRET level) identifying: Intelligence-assessed high-risk vendors/entities, concerning	Entities lack intelligence to identify vendors of concern. TISN classified briefing (quarterly updates on intelligence-assessed

jurisdictions/technologies, emerging supply chain threats, recommended mitigations -Entities integrate government-identified vendors of concern into assessment procedures—reduces individual entity intelligence burden	high-risk vendors/jurisdictions) reduces individual entity burden.
R8: Define "no practical alternative" determination methodology -Entity claiming sole-source must document for example: -Market research (contacted ≥5 potential suppliers globally), cost analysis (alternatives >200% cost premium), timeline analysis (alternatives >12 months qualification), technical feasibility (patent/proprietary constraints) -Sole-source claims >$5M require independent verification (auditor/government review) -3-year sunset clause—entity must revisit sole-source determination, demonstrate continued lack of alternatives or develop new source	"No practical alternatives" creates loophole that entities claim sole-source without adequate search. Documented methodology ensures legitimate sole-source determinations.
R9 Align Supply Chain 2 with mandatory government FOCI requirements	Harmonise Supply Chain 2 vendor assessment methodology with upcoming mandatory government ICT FOCI assessment Single assessment satisfies both government procurement and CIRMP Supply Chain 2 requirements Could publish joint guidance (Home Affairs + Finance) ensuring consistency, avoiding duplicative compliance

Supply chain measures: Regulatory impact analysis

Executive position

Supply chain 1: Supply chain vulnerability mapping.

Supply chain compromise represents a critical threat vector, and ACSC reporting that incidents affecting critical infrastructure frequently originate in the supply chain. Comprehensive vendor mapping enables identification of concentration risks, single points of failure, and potential vectors for supply chain attacks. The proposed requirements for sub-supplier visibility (tier 2+) and identification of critical software components is needed. However, achieving meaningful sub-supplier visibility faces significant practical limitations as most vendors treat sub-supplier relationships as commercially confidential, and contractual leverage to compel disclosure varies significantly.

For a representative of our clients, resource requirements: $150K-$500K for vendor assessment processes, supply chain mapping tools, vendor questionnaires, contract reviews, and ongoing documentation maintenance. 24 months realistic for comprehensive Tier 1 mapping; sub-supplier visibility may require 36+ months and remain incomplete for commercially resistant vendors.

Supply chain measure 2: Vendors of concern

Outside of financial clients or clients in highly regulated industries, it is not usual to see vendors of concern managed in risk management systems unless directly mandated by governments in which a client is operating in. Similarly to the response for FOCI measures, boards may simply 'accept the risk'. For clients who do not have a risk management system in place resource requirements: $80K-$200K for vendor risk assessment framework development, threat intelligence subscriptions, vendor assessments, and documentation processes. 18 months reasonable following government guidance publication. Depending on client maturity, limited access to classified threat intelligence; legal risk of vendor designation; commercial constraints when alternatives unavailable; contractual implications of vendor concern findings

Personnel security hazard measures

Personnel 1: Personnel security plan

Executive position

Support with critical definitional clarifications and sector-specific implementation guidance. Foreign Ownership, Control and Influence (FOCI) risks represent documented threat vectors requiring explicit regulatory attention, but the "minimise or eliminate as far as reasonably practicable" standard requires substantial interpretation where supply chain diversification is economically or technically infeasible.

Recommendations and Rationale

Recommendation	Rationale
R1: Define "critical worker" with objective criteria -For example, Critical worker = personnel (employees, contractors, vendors) meeting ANY: -Direct physical access to critical systems (OT, SCADA, control rooms, substations, treatment plants), privileged cyber access (domain admin, critical system accounts, security tool access, remote OT access), contractors/MSPs with equivalent access levels, senior decision makers -Exclude: Administrative staff without system access, non-privileged IT users	"Critical worker" undefined creates compliance ambiguity for example: SCADA tech vs. finance analyst, who qualifies? Objective criteria (i.e. direct system access OR privileged cyber access OR senior roles OR contractor equivalents) provides clear definition.
R2: Align personnel security plan requirements to PSPF standards or equivalent. -Mandate personnel security plan compliance with PSPF personnel security controls or equivalent maturity (or an equivalent control set from ISO27001 Annex A etc)	Enables cross-government consistency, leverages established framework, reduces entity burden reinventing personnel security programs
R3: Require Insider Threat Program framework adoption -Mandate personnel security plan incorporate insider threat program -(e.g. Maturity Framework elements: Dedicated insider threat function with executive visibility, information integration	Addresses behavioral insider threat vs. background checks alone (checks past history, monitoring detects current risk)

from HR/IT/security/legal stakeholders, monitoring user activity on critical systems, risk scoring for behavioral pattern recognition, investigation procedures with legal/privacy compliance, awareness training for personnel and managers)	
45: Establish structured offshore critical worker framework to include in a personnel security plan -Offshore critical workers (where onshore alternatives unavailable) require compensating controls like Access restrictions, enhanced monitoring, foreign equivalent clearance, contractual security obligations, quarterly ongoing reviews. - Suggest sole-source offshore contractors (no Australian alternatives) require an approval mechanism demonstrating exhaustive domestic search, alternative development plan, enhanced controls implementation	
R5: Define comprehensive personnel security plan minimum content -Mandatory elements could include: Critical worker identification methodology (criteria, position inventory), background checking procedures (pre-employment tiers, periodic revalidation, trigger events), physical access management (badging, escort requirements, access zones per Cyber 2), cyber access management (privileged access approval, least privilege, access reviews), insider threat program (behavioral monitoring, risk indicators, investigation process), security awareness training (annual minimum, role-specific for critical workers), incident response (security breach, insider threat investigation), offboarding (access revocation, exit interviews, credential return, non-disclosure)	Suggest selection of subset from PSPF (screening, monitoring, access management, insider threat, training, incident response, offboarding) ensures minimum baseline across all entities.
R6: Integrate personnel security plan with cyber controls -Personnel-cyber integration requirements: -Personnel vetting status gates cyber access provisioning—adverse AusCheck	Personnel security operates independently from Cyber 2-3 —missed integration. Personnel-cyber linking (vetting status gates system access, MFA logs feed insider threat analytics,

	cannot receive privileged access to critical systems, -qualified AusCheck requires enhanced monitoring + time-limited access, MFA authentication logs to feed insider threat analytics for anomalous access patterns -Access provisioning systems enforce pre-employment background check completion before account creation, periodic revalidation triggers access review (user whose background check expired loses critical system access until revalidated)	provisioning checks background status) creates defense-in-depth detecting threats missed by stand alone controls.

Personnel 2: Strengthening background checking

Executive position

Support with critical definitional clarifications and sector-specific implementation guidance. Foreign Ownership, Control and Influence (FOCI) risks represent documented threat vectors requiring explicit regulatory attention, but the "minimise or eliminate as far as reasonably practicable" standard requires substantial interpretation where supply chain diversification is economically or technically infeasible.

Recommendations and Rationale

Recommendation	Rationale
R6: Mandate continuous vetting and trigger event reassessment -Ongoing monitoring: Financial distress indicators (bankruptcy filings, garnishments, unusual expenses), security incident involvement (policy violations, system misuse, data breaches), foreign contacts/travel (unexplained trips >30 days, foreign national associations), criminal justice system contact (charges, arrests, restraining orders), behavioral concerns (substance abuse, workplace violence, performance degradation) -Trigger event reassessment within 30 days: Criminal charges/convictions, security	5-year revalidation inadequate—insider threat develops between checks (financial pressure, foreign recruitment, ideology shift). Could base on PSPF which requires ongoing monitoring; trigger event reassessment (criminal charges, foreign travel, financial distress) within 30 days detects emerging threats.

incident involvement, foreign travel >30 days to high-risk jurisdictions, bankruptcy/foreclosure, domestic violence charges	
R4: Implement risk-tiered background checking requirements -Tier 1 (high-risk: direct OT/critical cyber privileged access): Mandatory AusCheck or Australian Government security clearance NV1+ equivalent, 3-year revalidation -Tier 2 (medium-risk: elevated IT access, sensitive data): Police check + employment verification + identity check, 5-year revalidation Tier 3 (low-risk: administrative, limited access): Identity + criminal history check, 7-year revalidation Proportional to risk, reduces AusCheck burden for lower-risk roles, prioritizes resources on highest-risk positions	Linked to R1 – the definition of critical worker needs to be defined. Mandatory AusCheck for ALL critical workers treats high-risk SCADA tech same as low-risk admin Risk-tiered approach (Tier 1 AusCheck, Tier 2 police check, Tier 3 basic) proportional to risk per PSPF model, reduces burden.
R5: Recognise equivalent recent background checks -Corporate background checks meeting AS4811:2022 standards within 12 months transferable entity validates equivalency rather than re-checking -Australian Government clearances (baseline, NV1, NV2, PV) exempt for validity period.	Recent equivalent checks duplicated unnecessarily—contractor cleared 6 months ago re-clears for new entity. Equivalency recognition (AS4811:2022-compliant checks within 12 months) with a possible critical worker check database could eliminate duplication.
R9: Create interim access framework during AusCheck processing	3-8 week AusCheck processing creates staffing gaps, so a new critical worker waits or works unrestricted. Interim access (expedited baseline 1-2 weeks, temporary supervised access, full check continues) maintains operations while ensuring security.
R10: Integrate with Personnel 1 security plan requirements	Personnel 1 (security plan) and Personnel 2 (background checks) overlap.

Personnel security measures: Regulatory impact analysis

Executive position

Personnel security measures 1: Personnel security plan.

The requirement aligns with PSPF personnel security principles and addresses the reality that not all insider threats involve malicious intent; negligence, social engineering, and inadvertent compromise represent significant risk vectors. A documented personnel security plan enables consistent application of controls across the workforce lifecycle.

However, applying uniform personnel security measures across all staff creates disproportionate burden. Risk-based approach differentiating between staff with access to critical systems/sensitive information (critical worker not defined but sounds like a privileged user) and general workforce would provide better security outcomes with lower compliance costs and is considered in personnel security plans. For clients without a risk management system in place (like ISO27001) or do not have a dedicate role (like a Security Officer) resource requirements: Resource requirements: $60K-$150K for Integration with existing HR policies and systems; privacy considerations for monitoring; industrial relations implications for certain controls, policy development, staff training, background checking programs, and security awareness programs.

Personnel security measure 2: Strengthened background checking

This measure appropriately recognises background checking for staff with access to critical systems directly mitigates insider threats from individuals with undisclosed foreign intelligence connections, criminal histories, or financial vulnerabilities exploitable for coercion. This measure aligns with PSPF requirements for government personnel and addresses the reality that critical infrastructure represents high-value targets for foreign intelligence services.

The challenge lies in implementation infrastructure. Unlike government agencies accessing national security checking through AGSVA (Australian Government Security Vetting Agency), private sector entities lack streamlined access to comprehensive checking services. AusCheck provides limited checking scope. Enhanced checks examining foreign connections, financial vulnerabilities, and ongoing monitoring require either expensive private investigation services or expanded government infrastructure. Resourcing is dependent on the number of critical/privileged access holders in an organisation and the cost of AusCheck fees and processing of application (which usually can be managed by existing HR or Security Officer functions)

Personnel security measure 3: Enhancing personnel material risks

This measure appropriately recognises that personnel risks extend beyond initial vetting to encompass ongoing behaviours, security awareness, and response to social engineering. The ACSC identifies social engineering and phishing as primary initial access vectors in critical infrastructure compromises. However, the measure requires clearer articulation of what specific controls are required beyond background checking (Measure 2) and personnel security plans (Measure 1) to avoid ambiguity about compliance.

For clients, user access or acceptable use policies capture risk controls that are implemented in an organisation, and for organisations with risk management systems in place controls are captured. Additional costs would be to implement specific security content in user training

Physical and natural hazards

Physical 1: Physical security plan

Executive position

We support the inclusion of a physical security plan. We suggest the inclusion of physical threat assessments and a physical security incident reporting framework, such as a climate resilience assessment and physical sabotage threat assessment, with a physical security incident reporting framework. We also suggest extending supply chain measures to physical supply chain security and suggest integrating physical security in business continuity measures.

Existing frameworks such as ISO27001 Annex A Physical controls or the Physical Zone assessment based on AISO Technical Notes 1/15 can provide existing models to create an appropriate physical security control and process baseline.

Recommendations and Rationale

Recommendation	Rationale
R1: Mandate comprehensive physical security plan -Require responsible entities develop physical security plan within CIRMP addressing: Physical security perimeter definition, access control systems (employee, visitor, contractor), perimeter protections (fencing, barriers, lighting), surveillance systems (CCTV coverage,	No mandatory physical security measure despite intelligence on nation-state actors "mapping and targeting" infrastructure. PSPF physical security domain and ISO 27001 Physical controls provide established frameworks—adoption creates baseline,

monitoring protocols), intrusion detection and alarm systems, physical security incident response -Implement visitor and contractor access management controls -Mandate minimum requirements: Pre-approval for access to sensitive areas (control rooms, OT facilities, communications hubs), escort requirements (visitors to critical areas must be accompanied by vetted employee), identity verification (government-issued photo ID, pre-registration for expected visitors), access logging (visitor register, badge tracking, duration monitoring), technology restrictions (no cameras, phones, recording devices in critical zones), extended access vetting (visitors/contractors >5 visits or >40 hours annually undergo background check)	prevents physical access vector bypassing cyber controls. Compliance with PSPF physical security domain, ISO 27001:2024 Annex A Physical, ASIO Technical Notes 1/15 or ACSC ISM physical security guidance
R2: Require climate resilience and natural hazard assessment -Mandate natural hazard and climate adaptation assessment identifying: -Primary natural hazards (bushfire, flood, extreme heat, cyclone, coastal erosion, landslide) based on asset location, climate change projections (increased frequency/intensity over 20-30 year asset life), vulnerability assessment (which assets exposed, criticality if damaged/destroyed), adaptation measures (engineering solutions, operational changes, insurance), contingency plans (alternative supply routes, backup systems, mutual aid agreements) -Update assessment every 5 years incorporating latest climate science, post-incident (within 90 days of major natural hazard event affecting region)	Climate change increasing bushfire/flood/heat risks — Australian critical infrastructure highly exposed (energy transmission, water treatment, transport). Mandatory climate resilience assessment ensures adaptation, protects long-lived assets (20-30 year lifespan) against evolving risks. Aligns with global climate-resilient infrastructure best practices
R3: Integrate physical and cyber security controls	Linked to R1

- Mandate physical-cyber integration requirements: - Physical access to critical system locations (OT control rooms, server rooms, SCADA facilities) subject to Personnel 2 background checks, physical access control systems (badges, biometrics) integrated with Cyber 3 MFA authentication logging, physical access to air-gapped critical systems (Cyber 2 segregated networks) logged and monitored equivalently to remote access, surveillance systems (CCTV) provide audit trail for critical system physical access investigations	Cyber measures (network segregation, MFA) address digital access but physical access to OT/SCADA systems bypasses all digital controls. Integration (physical access requires background check + logged equivalently to remote access) creates defense-in-depth, prevents Volt Typhoon-style pre-positioning via physical vector.
R4: Adopt risk-tiered physical security framework for distributed infrastructure For example: -Tier 1 (major control centers, critical generation/treatment plants, primary substations): Comprehensive controls—secure perimeter (fencing, barriers), manned access control, CCTV with 24/7 monitoring, intrusion detection, armed response arrangements -Tier 2 (regional facilities, secondary sites): Standard controls—perimeter fencing, access control (electronic locks), CCTV (recorded, not live-monitored), intrusion alarms, periodic security patrols -Tier 3 (distributed remote assets, poles/towers, rural pump stations): Basic controls—locked enclosures, tamper detection sensors, periodic inspections (monthly-quarterly)	Energy/water/transport operate hundreds of distributed remote sites—impossible to secure all. Risk-tiered approach (Tier 1 comprehensive, Tier 2 standard, Tier 3 basic) proportional to criticality and feasible for distributed infrastructure, prevents under-protecting critical sites or over-investing in low-risk sites.
R5: Require physical sabotage threat assessment -Physical security plan must include sabotage risk analysis: -Identify critical single points of failure (key substations, major treatment facilities, critical bridges/tunnels), assess sabotage consequences (service disruption duration, population	Intelligence emphasises threats but sabotage risks not assessed. Historical substation attacks, transmission tower vandalism demonstrate vulnerability. Sabotage assessment identifies critical single points of failure requiring enhanced protection

affected, cascade to other sectors, economic impact), prioritise highest-risk assets for enhanced physical protection (top 10-20 critical nodes)	(vehicle barriers, setback zones, hardening).
R6: Implement visitor and contractor access management controls Mandate minimum requirements: Pre-approval for access to sensitive areas (control rooms, OT facilities, communications hubs), escort requirements (visitors to critical areas must be accompanied by vetted employee), identity verification (government-issued photo ID, pre-registration for expected visitors), access logging (visitor register, badge tracking, duration monitoring), technology restrictions (no cameras, phones, recording devices in critical zones), extended access vetting (visitors/contractors >5 visits or >40 hours annually undergo background check)	Linked to R1. Some places have this in an access policy Personnel measures address critical workers but thousands of contractors/visitors access sites—unvetted physical access creates insider threat. Visitor management (pre-approval, escorts, logging, technology restrictions) addresses threat vector from third parties.
R7: Create physical security incident reporting framework -Expand SOCI Act incident reporting to include physical security breaches: Unauthorized access (tailgating, forced entry, bypassed access controls), perimeter intrusions (fence breaches, trespassing), suspicious surveillance (photography, drone overflights, social engineering), physical attacks (vandalism, sabotage attempts, weapons found), theft (critical components, credentials, access devices) -Reporting timeline: Critical incidents (active breach, immediate threat) within 12 hours, significant incidents (successful unauthorized access, confirmed surveillance) within 72 hours	Cyber incidents reportable under SOCI but physical breaches not captured. Physical incident reporting (unauthorized access, surveillance, attacks) enables national threat picture, patterns across entities signal coordinated reconnaissance, triggers sector warnings.
R8: Extend supply chain measures to physical supply chain security -Supply Chain 2 vendor assessment expanded to include: -Vendor facility physical security (manufacturing sites, warehouses meet minimum standards), tamper-evident packaging (critical components sealed, tamper indicators), chain of custody documentation (components tracked	Supply Chain 2 addresses FOCI but solar inverter case study involves physical supply chain compromise ("unexplained communication equipment"). Physical supply chain security (vendor facility standards, tamper-evident packaging, receiving inspection) addresses

	from manufacture to installation), receiving inspection procedures (visual inspection, testing for counterfeits/modifications, quarantine suspect items), secure storage (critical spares in access-controlled areas, inventory auditing)	counterfeit/tampered components.
R9: Clarify physical security and business continuity integration -Physical security plan and natural hazard assessment must integrate with business continuity management:		
Physical controls reduce disruption likelihood (perimeter security prevents sabotage, climate adaptations reduce natural hazard damage), natural hazard scenarios inform business continuity planning (flood evacuation procedures, bushfire response protocols, heat wave operational restrictions), recovery procedures address both malicious and natural events (facility damage assessment, alternative operations, mutual aid activation)		Natural hazards impact business continuity but integration unclear.

Appendix

Appendix A: Mapping of SOCI sectors to globally relevant standards

Executive position

Noting our recommendation for more defined control sets that cover OT elements of Operator assets, we have created mapping of common international and national standards which provide a starting point for sector specific control advisories at minimum to implement.

Recommendations and Rationale

Table 1: SOCI sector mapped to common global standards

Sector	Common global standards
Communications	ISO/IEC 27001 (ISMS), ISO/IEC 27002 (controls), NIST CSF, ITU-T X.1000-series (telecom-specific security), IEC 62443 (for OT-like network-control systems).
Data storage or processing	ISO/IEC 27001, ISO/IEC 27017 (cloud), ISO/IEC 27018 (cloud privacy), ISO/IEC 27701 (privacy extension), NIST CSF, NIST SP 800-53, ISO 27002 controls
Defence industry	DSPF, ISO/IEC 27001, NIST CSF, NIST SP 800-171 (for US-linked defence supply chains), ISO 27002, IEC 62443 (for IACS/OT in defence plants), national-specific cyber-security frameworks (e.g., ASD Essentials, UK NCSC guidance).
Higher education and research	ISO/IEC 27001 (whole-organisation ISMS), ISO 27002, NIST CSF, NIST SP 800-171 (for sensitive research), sector-specific research-security frameworks (e.g., RENIS-NZ, NITRD).
Energy	ISO/IEC 27001, ISO/IEC 27019 (sector-specific), IEC 62443 (for power-generation and grid-control systems), NERC CIP (North America), NIST CSF, ENISA OT-ICS guidance.
Financial services and markets	ISO/IEC 27001, ISO 27002, PCI DSS (for payment systems), NIST CSF, ISO 22301 (BCMS), sector-specific prudential-security frameworks (e.g., APRA CPS 234 in Australia).
Food and grocery	ISO/IEC 27001 (for corporate IT and supply-chain systems), ISO 27002, ISO 22000 (food safety, with security-adjacent controls), IEC 62443 (for OT/SCADA in processing plants), NIST CSF.
Healthcare and medical	ISO/IEC 27001, ISO 27799 (health-specific controls), ISO 27002, ISO 27018 (health-related privacy), NIST CSF, IEC 62443 (for OT/medical-device-related control systems).

Space technology	ISO/IEC 27001, ISO 27002, NIST CSF, space-specific security frameworks (e.g., ECSS-S-ST-01-11, NIST CSF-space-profiles), IEC 62443 (for ground-station and mission-control OT).
Transport	ISO/IEC 27001, ISO 27002, NIST CSF, sector-specific frameworks (e.g., ICAO-aviation-cyber, IMO-cyber, rail-specific cyber-guidelines), ENISA OT-ICS guidance, IEC 62443 for OT/SCADA in ports, rail signals, and terminals.
Water and sewerage	ISO/IEC 27001, ISO 27002, ISO 27019 (adapted for water), IEC 62443 (for SCADA, pumping, and treatment-plant OT), NIST CSF, ENISA OT-ICS guidance.

Rationale

All ISO/IEC management systems are risk management systems at their core – it is the engine which drives them in practice.

In practice, most regulated SOCI entities in Australia use ISO/IEC 27001 as the core information security management system (ISMS), layer IEC 62443 or ISO 27019 for OT-heavy systems, then apply NIST CSF-style risk-management and sector-specific mandates (e.g., NERF CIP-style expectations for energy, or APRA-style cyber-resilience for finance).

Appendix B: Mapping of differences in security frameworks and maturity models in SOCI Act

Executive position

The security frameworks outlined in SOCI Act for RMP compliance are not like-for-like and present a coverage concern. In coverage, ISO 27001 and NIST CSF are comprehensive across all security domains; Essential 8 covers only the most critical technical controls in Windows-based systems; and C2M2/AESCSF focus on measuring operational maturity in critical infrastructure environments.

ISO 27001 is a comprehensive management system with certification (what you must build). Essential 8 are targeted technical controls (what you must do right now) for Microsoft -based systems. NIST CSF is a flexible guidance framework (how to think about cybersecurity). C2M2 is a maturity measurement tool (how mature are you?) Finally, the AESCSF is cector-specific Australian energy framework (C2M2 tailored for Australian energy combining Essential 8 and local requirements)

Recommendations and Rationale

Table 2: Comparison of choice of security frameworks to comply with SOCI Act

Framework	ISO27001	Essential 8	NIST CSF	C2M2	AESCSF
What it is	International standard for Information Security Management Systems (ISMS)	Set of 8 technical controls to prevent common cyber attacks	Flexible cybersecurity risk management framework	Maturity assessment tool to measure cybersecurity capability progression	Sector-specific framework for Australian energy sector
Origin	International (ISO/IEC)	Australian (ASD)	US Government (NIST)	US Dept of Energy	Australian (AEMO + ACSC), based on C2M2
Purpose	Establish a complete, auditable security management system with governance and risk-based approach	Mitigate the most common cyber threats (ransomware, phishing, system compromise)	Guide organisations to manage cybersecurity risk across any sector	Benchmark and measure cybersecurity maturity over time; identify gaps and prioritise improvements	Enable energy sector organisations to assess and improve cyber maturity in Australian context
Structure	93 controls in Annex A, organised into 4 themes (Organisational, People, Physical, Technological controls)	8 mitigation strategies: - Patch applications - Patch OS - Multi-factor auth - Restrict admin - App control - Restrict macros	6 core functions: - Govern - Identify - Protect - Detect - Respond - Recover	10 domains with 350+ practices, mapped to Maturity Indicator Levels (MIL 0-3)	11 domains (10 from C2M2 + Australian Privacy Management), with 282 practices and anti-patterns across 3 Security Profiles

		- User training - Backups			
Scope	Enterprise-wide; covers governance, processes, technical and organisational controls	Technical controls only; focused on preventing known attack vectors	High-level framework applicable across all industries and risk profiles	Self-assessment across entire organisation; designed for critical infrastructure and energy sectors	Energy, gas, and liquid fuel sectors; includes IT and OT environments with Australian policy alignment
Certification /Compliance	Yes , requires formal third-party audit and 3-year certification cycle	No formal certification, but compliance often required by government or clients	No, voluntary framework; no certification or audits required	No, self-assessment tool; no certification	No, voluntary framework, but may be mandated by Australian regulators or AEMO for energy participants
Flexibility	Moderate, you select applicable controls via risk assessment, but full ISMS process is mandatory	Low, prescriptive set of 8 mandatory controls with defined maturity levels (0-3)	High, highly adaptable to your organisation's risk profile and existing frameworks	High, organisations choose target maturity levels based on risk and priorities	Moderate, designed for energy sector but allows tailoring within Security Profiles
Primary focus	Governance, policies, continuous improvement, and documentation	Technical mitigation of real-world attack techniques	Risk management and cyber resilience across Identify-Protect-Detect-Respond-Recover lifecycle	Measuring maturity and continuous improvement using "crawl-walk-run" progression	OT/ICS-heavy energy infrastructure with Australian regulatory alignment (Essential 8, Privacy, NDB)
Implementation Timeline	6-18 months for full ISMS and certification	3-6 months for initial controls; maturity uplift takes longer	Varies; can start immediately and layer on over time	Ongoing, designed for periodic self-assessment (annual or biannual recommended)	6-12 months depending on current maturity and target Security Profile
Use case	Organisations needing international certification, customer trust, or regulatory proof of compliance	Rapid baseline security uplift; mandated for Australian government contractors and many critical infrastructure entities	Organisations wanting flexible, risk-based guidance that can be integrated with other frameworks (ISO, NIST, Essential 8, etc.)	Critical infrastructure operators (especially energy, water, transport) wanting to benchmark maturity and track improvement	Australian energy operators (electricity, gas, liquid fuels) needing to meet AEMO or government expectations aligned with C2M2
Key difference in simple terms	You must establish an auditable management system	Do these 8 overarching catergories to stop 85% of attacks	Here's a way to think about managing cyber risk, customise as needed	Where are you now on a 0-3 scale, and where do you want to be?	Here's how energy sector entities in Australia should assess OT/IT cyber maturity

Relationship to others	Can include Essential 8 controls within its technical controls	Often implemented as part of ISO 27001 ISMS technical controls	No, voluntary framework; no certification or audits required	AESCSF is built on top of C2M2 structure; complements NIST CSF by adding maturity measurement	Incorporates Essential 8, aligns with NIST CSF and ISO 27001, and uses C2M2 maturity model