agilient
Security Risk & Resilience

INFORM · ASSESS · PROTECT

CRITICAL INFRASTRUCTURE COMPLIANCE · SOCI ACT

Enhanced CIRMP Rules: what operators must do by mid-2027

The Enhanced CIRMP Rules commenced in June 2026, moving the Critical Infrastructure Risk Management Program from principles to prescriptive, evidence-based controls for nine critical infrastructure asset classes. Obligations are staged, and the first deadlines fall in mid-2027.

WHAT THE ENHANCED RULES NOW REQUIRE

Cyber and information security

- Phishing-resistant multi-factor authentication with central logging
- Network segregation, with critical systems able to run for three months while others are restored
- Uplift to a higher framework maturity level (AESCSF for the energy sector)

Personnel and supply chain

- AusCheck check or Negative Vetting 1 for critical workers, reassessed at least every five years
- Access management for unauthorised access and credential misuse
- Supplier mapping, FOCI and sanctions checks, and set outage thresholds

Physical and material risks

- Holistic, centrally managed physical security plan across all hazards
- FOCI, offshore or remote access, and national-security impairment
- Board-approved and annually reviewed risk management program

WHICH SECTORS ARE CAUGHT

Energy
Electricity, energy market operator, gas and liquid fuel assets.

Water
Critical water assets.

Broadcasting
Critical broadcasting assets.

Domain name system
Critical domain name system assets.

Freight
Freight infrastructure and freight services assets.

BY THE NUMBERS

9
critical infrastructure asset classes now in the enhanced tier.

12 mo
to the first deadline (mid-2027): additional material, core cyber and access-management risks.

24 mo
to full compliance (mid-2028): MFA, network segregation, vetting, supply chain and physical security.

3 mo
that critical systems must keep running while other systems are restored.

WHAT OPERATORS SHOULD DO NOW

- ✓ **Run a gap analysis.** Test the current CIRMP against the enhanced requirements, category by category.
- ✓ **Identify FOCI exposure.** Assess ownership, suppliers and data for offshore or remote access.
- ✓ **Scope the physical security plan.** Cover access control, monitoring and the physical consequences of cyber and supply chain hazards.
- ✓ **Map the critical workforce.** Plan AusCheck vetting early, as the reassessment cycle takes time to establish.
- ✓ **Map the supply chain.** Identify major suppliers and critical components, and set outage thresholds.
- ✓ **Secure board endorsement.** The CIRMP is board-approved and the investment is material.

For each hazard area, can the organisation show a regulator **the evidence that the risk is being managed**, and if not, the plan and date to close the gap?

agilient.com.au
CRITICAL INFRASTRUCTURE · SOCI · RISK ASSESSMENT

Sources: Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (F2026L00701), legislation.gov.au; Cyber and Infrastructure Security Centre, cisc.gov.au. Point-in-time as at July 2026; verify against the primary source before formal use.