

CIRMP Assurance: Internal Review vs. Independent Third-Party Audit

Every responsible entity with a Critical Infrastructure Risk Management Program (CIRMP) must submit an annual report within 90 days of the end of the financial year (28 September for most entities). The CISC's online form now asks the board to declare which assurance approach underpins the report: internal review, or an independent third-party audit. Neither is mandatory by law - but the choice has real implications for what evidence sits behind the board's sign-off.

Core reporting requirements

- **Currency:** A declaration that the CIRMP was up to date at financial year-end.
- **Incidents:** Details of any incidents with a significant relevant impact on the asset.
- **Variations:** An outline of any changes made to the CIRMP during the year.
- **Effectiveness:** An evaluation of the program's effectiveness in mitigating hazard impacts.
- **Attestation:** Confirmation the report was approved by the board or governing body.

Internal Review vs. Independent Audit

	Internal Review	Independent Third-Party Audit
Who performs it	Internal risk, security or compliance function	External assessor with no operational stake in the outcome
What it evidences	That a review took place and the program was assessed	That the CIRMP is operating effectively in practice - governance, risk coverage, evidence and control effectiveness
Board confidence	Relies on internal judgement and existing knowledge of the environment	Provides an external, defensible line of evidence for Section 180 due-diligence obligations
Typical gap exposed	Asset visibility and OT/IT boundary assumptions often go untested	Needs lead time - scoping and evidence-gathering can't start the week before lodgement
Cost / effort	Lower direct cost; uses existing staff time	Higher direct cost; typically weeks, not days, if scoped properly

Board Governance & Director Liability

Approving the CIRMP annual report engages directors' individual obligations under Section 180 of the Corporations Act 2001 - the duty of care and diligence. An independent review gives the board an external, structured line of evidence to point to if that duty is ever tested, rather than relying solely on management's self-assessment.

Consequences of Non-Compliance

- **Section 30AG:** failing to lodge the board-approved annual report carries up to 150 penalty units for a body corporate.
- **Section 30AC:** failing to maintain a compliant CIRMP carries up to 200 penalty units.
- **False or misleading information** is a separate matter under the Criminal Code, not a civil penalty.
- **No extensions:** the SOCI Act does not provide for exemptions to the 90-day window.

Pre-Submission Governance Checklist

- Can we point to evidence of every asset connected to the OT network, not just the ones we assumed were in scope?
- If challenged, does our assurance approach hold up as independent, or does it rely on the same people who built the program?
- Is there enough lead time left to commission an independent review before board sign-off, if needed?

This document is provided for informational purposes only and does not constitute a formal compliance opinion. Entities should seek tailored guidance from a qualified legal or compliance advisor regarding their specific obligations.

