SOCI Enforcement is Here, Proof Is Mandatory

Turning SOCI compliance from burden into a commercial asset for Australia's renewables sector

ASE TECH
Ask Solve Evolve

The SOCI enforcement era is here - but it's also an opportunity

Australia's renewable energy sector has entered the enforcement era of the Security of Critical Infrastructure (SOCI) Act. The days of education and guidance are over. Regulators are now investigating, auditing and applying penalties to operators whose critical infrastructure risk management plans (CIRMPs) are found to be in breach, as well as the directors who sign off on them.

Where once critical infrastructure CIRMPs could be filed and forgotten, the Federal Government's Cyber and Infrastructure Security Centre (CISC) is now issuing formal notices and sending investigators on-site to test whether programs are understood and effective. Operators need to demonstrate not only that controls exist, but that they are embedded across every site and every asset.

Meanwhile, boards are now in the third cycle of attestations under the SOCI Act. Each cycle is a legal assurance that the operator's risk management program is documented and operating as intended. If that assurance proves false, directors face direct liability, including possible criminal penalties.

Portfolios have grown quickly through new developments and acquisitions, leaving operators with assets built to different standards and maintained by different vendors. A CIRMP may look complete on paper, but if controls like segmentation, remote access or supplier oversight vary from site to site, both the organisation and its leaders are at risk.

"Trial audits found two-thirds of entities still carried compliance gaps."

The key message for Australia's renewable energy leaders is compliance does not equal protection; and that reality is being tested. Audits mean little if the regulator finds gaps between what's documented, and what's happening on-site. Yet compliance doesn't have to be a burden. Built well, a CIRMP becomes living due diligence: proof that assets are resilient, revenue is protected and investors can trust in their value.

That's the lens ASE Tech brings. We help operators in the renewable energy sector to close the gap between paperwork and practice, so compliance strengthens operations and protects asset value, instead of weighing the business down.

This report is designed to help sector leaders navigate the toughest compliance test in years, and to offer practical guidance on turning those challenges into a competitive edge.

Andrew Sjoquist
CEO
ASE Tech

Audit ready, regulator exposed

Many operators in the renewables sector are still only “surface ready” for SOCI compliance. They look prepared and the paperwork is in order, but CISC audits are already uncovering gaps between documentation and practice. If staff on-site cannot explain to investigators how controls are applied, or if basic measures are inconsistent, the protection is superficial.
When the regulator comes knocking

CISC is now actively auditing operators. Operators are being selected at random, or flagged by incidents and inconsistencies. With just two weeks’ notice, you will be expected to prove your CIRMP in practice, with investigators testing staff, controls and procedures on-site.

If gaps are found, the regulator can issue enforceable directions or escalate to penalties. The safest position is to assume you are on the list, and prepare as if the knock on the door could come at any time.

The weak spots regulators are finding

Generally, the blind spots CISC is uncovering are not complex technical problems. Some of the most common we see include:

- Inconsistent background checks on critical workers
- Contractors given access without proper vetting
- Flat networks that let an intruder move freely once they are inside
- Suppliers signing contracts without proving they meet SOCI standards
- Outdated devices left unpatched
- Unsecured modems still plugged in

A common misconception is treating SOCI as a cyber-only obligation. In reality, CIRMP must cover every domain: cyber, personnel, physical and supply chain. Regulators are already finding that over-reliance on a single supplier, weak access controls, or poor worker vetting can create just as much liability as a technical flaw.

These are the kinds of exposures that CIRMPs might skim over, but the regulator will not. And they are the very risks that board members are now personally attesting have been addressed. At that point, surface-level compliance on paper is a direct liability.

Just as safety evolved beyond compliance to become part of culture, asset security is on the same path. No one today describes OHS/WHS as a tick-box exercise. Security of critical infrastructure is undergoing the same transformation.

Viewed differently, though, the same framework can be treated as an investment. A well-built CIRMP acts as a form of continual due diligence. Not only does it help to strengthen operational resilience, it also protects revenue and increases the long-term value of the asset.

Closing these gaps requires an ecosystem of operators, contractors and partners all aligned to the same standards. A single weak link can leave an entire portfolio exposed.

The real cost of non-compliance

- **Directors:** A false attestation is a criminal offence. Penalties can include fines and jail time. Liability is personal.
- **Operators:** Breaches can attract fines of up to $222,000 per contravention, plus enforceable directions from the regulator.

"If you think of CIRMP as just a report that gets filed away in a drawer, you're missing the point. It is about making sure assets are genuinely secure in a constantly changing landscape."

– Senior renewables executive,
speaking at a recent ASE Solve Virtual Event.
Watch here

Where renewables face the hardest test

Geography was once the biggest compliance challenge for renewable operators. Assets are usually spread across regional and remote sites, and getting a stable connection into every farm or facility was hard enough. That challenge is still there, but it's no longer the hardest one.

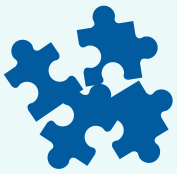
Today, the greater test is portfolio diversity. Most are a mix of old sites, new builds and acquisitions, each with its own vendors, systems and vulnerabilities. Small in-house teams are stretched across dozens of assets, and keeping basic IT hygiene consistent across all sites is almost impossible.

Retrofitting controls later is costly and often incomplete. The longer security is delayed, the more "technical debt" builds up, which leaves operators with vulnerabilities to patch across assets designed to different standards. With renewable facilities expected to operate for up to 35 years, small oversights today become major liabilities tomorrow.

On top of that, many renewable operators rely heavily on contractors and service providers. That creates even more gaps in visibility, and the regulator has already flagged that supply chain accountability will be under the microscope in the next enforcement cycle. Meeting that test will demand an ecosystem approach, where contractors and service providers are held to the same standard as operators themselves.

Meanwhile, the rules themselves are still evolving. Compliance is a moving target, which makes proving consistency across such a fragmented environment harder than ever.

Renewables' Big 3 SOCI challenges



Mixed Portfolios

Legacy sites, new builds and acquisitions all running different standards

Stretched Internal Teams

Few staff stretched across dozens of sites, struggling with basic IT hygiene.

Supply Chain Gaps

Heavy reliance on contractors, with accountability now under regulator scrutiny.

The fix: Treat CIRMP as a living framework, apply consistent controls across every site and hold contractors to the same standard you hold yourself.

A de-risked asset is a valuable asset

While many view CIRMP preparation as a regulatory burden, it can also be a powerful commercial tool. Built properly, a CIRMP acts as rolling due diligence that de-risks your asset and raises enterprise value.

Well-documented, operational controls add tangible value in M&A and investment contexts. They prove that risks are understood and managed, which strengthens the case for higher valuations and investor confidence.

The financial stakes are real

Consider a solar farm generating $8 million a year. If that farm is taken offline for just a week, whether from a cyber incident or a regulator-imposed shutdown, the lost revenue is around $150,000. Stretch that outage to a month and the loss climbs past $650,000.

Either way, the impact dwarfs a $222,000 SOCI fine. The regulator may issue the penalty once; the market punishes you every day the asset isn't producing. For operators working under thin margins, every hour of lost production cuts directly into returns. Boards will not invest in "compliance" for its own sake, but they will back resilience when the revenue at risk is clear. CIRMP investment is not a sunk cost; it is insurance against downtime and a lever for preserving enterprise value.
rcise. Security of critical infrastructure is undergoing the same transformation.

"Boards don't fund compliance. They fund resilience."

Turning compliance into value
A well-built CIRMP forces operators to tighten the basics: clear visibility of every asset, consistent maintenance, accountability across suppliers. That same discipline delivers efficiency gains as well as risk reduction.
Even a marginal improvement in availability or output has a real financial impact. On a $40 million portfolio, a 1% gain equates to $400,000 a year. In other words, when compliance is embedded in daily operations, it both reduces risk and generates return.

Benefits of a de-risked asset

- **Investor confidence –** stronger financial and risk profile.
- **Insurance costs come down –** better protection means cheaper cover.
- **Asset stays productive –** less downtime means more yield.
- **Reputation builds trust –** reliable operators win more business.

The new standard for SOCI compliance

The days of annual, paper-based compliance are over. A CIRMP that sits on the shelf is now a liability. Regulators can test in real time whether controls are operating as attested. A static plan is soon out-of-step with what's happening on-site, leaving operators and their directors exposed when CISC comes to check.

A stronger model is continual compliance. Instead of waiting for the next audit, operational checks are embedded into daily routines and mapped directly to governance and compliance requirements. That way, operators know at any point in time whether their controls are holding. Most importantly, they can prove it when the regulator asks.

Continual compliance takes an ecosystem

No operator can meet SOCI obligations alone. Continual compliance demands an ecosystem of support:

- Operational partners who understand critical infrastructure
- Governance specialists who turn obligations into workable frameworks
- Compliance advisers who ensure reporting stands up to scrutiny

Effective partnerships go beyond advice. They integrate directly into core processes - from HR onboarding to supply chain procurement - so compliance is embedded in everyday workflows, rather than introduced after the fact. The strongest results come when operators, service providers and suppliers work in lockstep, closing gaps collectively rather than pushing them downstream. This way, the organisation always knows where it stands.

For renewable operators, the real benefit of this approach is building a clear line of sight from daily operations to board-level assurance. If CISC arrives, you can show evidence on the spot. If investors ask, you can demonstrate that controls are embedded and understood.

Key takeaways for operators and directors

- Treat compliance as a daily discipline, not a once-a-year project.
- Make sure staff and contractors can explain how controls work.
- Keep evidence current and accessible, so you are always audit-ready.
- Choose partners who can work seamlessly alongside your teams and other ecosystem partners.

From Annual Audit to Continual Compliance

Old Model
Annual Audit

- **Static –** CIRMP filed once a year
- **Outdated –** controls change within weeks
- **Reactive –** gaps found only at audit
- **High risk –** paper ≠ protection

New Model
Continual Compliance

- **Dynamic –** daily operational checks
- **Current –** evidence always up-to-date
- **Proactive –** gaps closed before audit
- **Resilient –** compliance embedded in operations

Partner ecosystem
operational - governance compliance

The SOCI readiness test

These are the behaviours that build resilience, and the habits that leave operators exposed. The mindset shift mirrors the way safety became embedded in operations: once treated as a compliance matter, now inseparable from daily practice.

Focus area	✓ Leaders	✗ Laggards
Scope	Treat SOCI as a multi-domain obligation, embedding controls across cyber, personnel, physical and supply chain.	Focus narrowly on cyber while leaving other domains exposed.
Security	Build controls in at the design stage of new projects; security is part of the blueprint, not an afterthought.	Leave security until energisation day, accumulating technical debt that is expensive and risky to fix later.
Mindset	Treat CIRMP as commercial stewardship: evidence of resilience revenue protection and asset value.	See compliance as a sunk cost and a box to tick for regulators.
Partnerships	Engage operational, governance and compliance partners early, and keep roles connected.	Rely on service providers without oversight or accountability.
Continuity	Maintain continual compliance with daily checks mapped to obligations; always audit-ready.	Depend on annual audits and static plans that are out of date within weeks.
Supply chain	Hold contractors and vendors accountable, demanding evidence they meet SOCI standards.	Assume suppliers comply without proof or monitoring
Lifecycle	Standardise designs and manage systems over the full lifecycle; controls are consistent across assets.	Accept one-off builds with inconsistent standards and poor patching or monitoring.

SOCI enforcement is here, the time to act is now

Australia's renewables sector has entered the enforcement era of SOCI. Regulators are past the education stage. Operators can now expect audits, investigations and penalties if requirements are not met.

The grace period has ended. Regulators are now testing the quality of CIRMPs, not just their existence, and requiring treatment action plans where gaps are found. Obligations are also extending into service providers, and the first enforcement actions are already emerging.

The onus is on operators to prove that the controls in their CIRMP are consistent, embedded and able to stand up under scrutiny. Acting early not only shields directors from liability, it protects millions in annual revenue and demonstrates the resilience that enhances enterprise value. When done well, it becomes a commercial asset, helping to drive investor confidence and setting up portfolios for long-term growth.
Passing a CIRMP audit is just the starting point. Continual compliance takes an ecosystem of operators, suppliers and partners all working to the same standard. Leaders who embrace this approach are turning CIRMP into a living framework - one that protects the enterprise today and builds confidence for tomorrow.

The ASE Tech perspective

ASE Tech has been part of Australia's critical infrastructure ecosystem for over two decades. In the renewables sector, our role is to connect operational, governance and compliance disciplines so operators can achieve continual compliance across diverse portfolios.

Unlike most partners, we do so from the inside out. As a licensed carrier, we are ourselves subject to SOCI enforcement, facing penalties as tough, and in many cases tougher, than those applied to our customers. That dual role, both regulated under SOCI and supporting those regulated by it, gives us a unique position inside the ecosystem. It's why we design and operate systems that are resilient by design, proven in practice and accountable at every level.

In the enforcement era, that perspective makes the difference between surface compliance and proven resilience.

“Owners can’t delegate this downstream. Ultimately, it is your asset, your money and your responsibility if it gets shut down.”

– Senior leader in the renewables sector,
speaking at a recent ASE Tech Solve Virtual Event.
Watch here

Ready to get started?

Book a call with an ASE Tech expert to turn your CIRMP into a driver of resilience and growth.