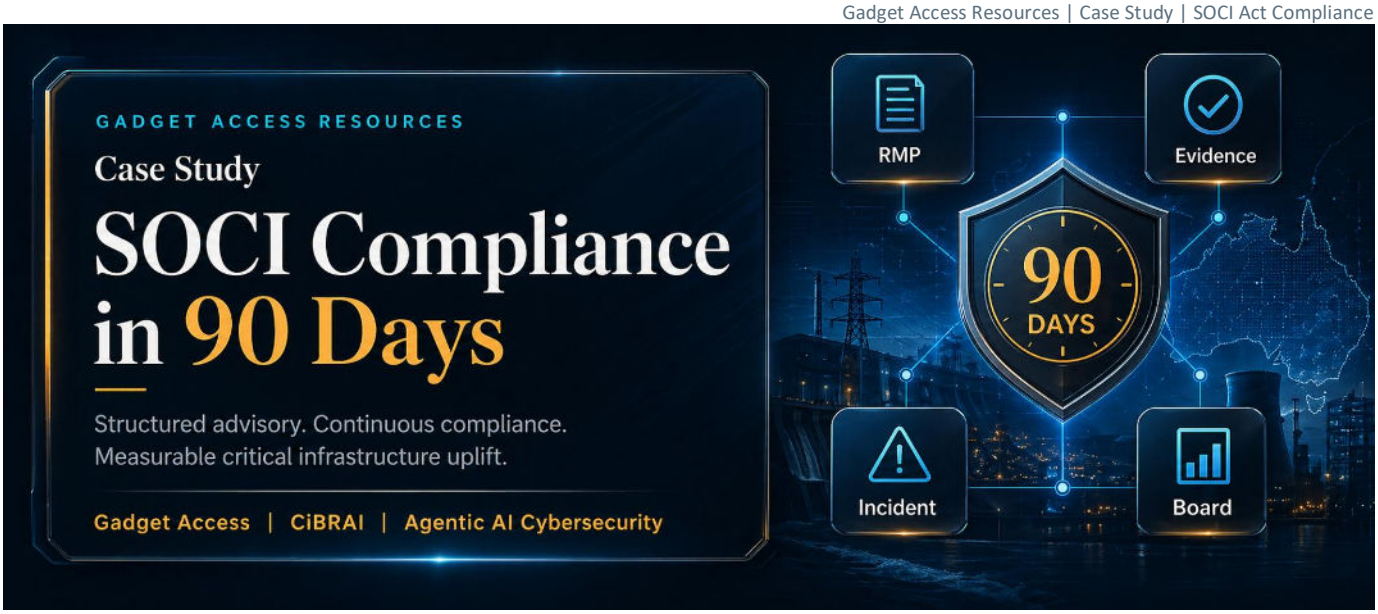

Critical Infrastructure Operator Achieves SOCI Act Compliance in 90 Days

How a structured advisory engagement delivered regulatory compliance alongside measurable security uplift.

Anonymised case study note: This case study is based on a structured advisory pattern for a critical infrastructure operator. Sector identifying details and metrics have been generalised to protect operational confidentiality, but the governance model, control uplift approach and outcomes are realistic for SOCI Act programs.

The 90 day problem

Critical infrastructure compliance tends to arrive in a deceptively simple wrapper. There is an Act. There are obligations. There is a deadline. How hard can it be? In practice, the organisation that called Gadget Access had the familiar ingredients: dedicated operational staff, several security products, decent policies, a board that cared, and a highly practical problem. Nobody could prove the whole picture quickly.

If SOCI is treated as a paperwork exercise, it will punish the operator later. The Risk Management Program obligation expects a written program, yes, but the hard parts are understanding material risk, interdependencies, suppliers, critical components and evidence. The regulator's question is never only "have you written a document?" It is "can you show you are managing risks to essential services as business as usual?"

The operator's challenge

The client operated essential services across geographically dispersed sites, with corporate IT, operational technology, cloud workloads, outsourced network services and a long tail of specialist providers. As with many Australian infrastructure operators, its estate had been assembled over years of sensible operational decisions. Sensible does not always mean tidy.

The asset inventory was close in some areas and heroic in others. Vulnerability records lived in one platform, network diagrams in another, supplier risk documents in procurement, incident playbooks in a shared drive and board reporting

in carefully polished monthly packs. Everyone was working hard, but hard work was being converted into fragments rather than assurance.

The SOCI pressure points were specific: confirm obligations and responsible roles, align the Risk Management Program to all four hazard vectors, establish evidence for cyber and information security controls, identify material risks and critical components, define data storage notification obligations, prove incident reporting readiness and build a board approved annual report pack. The team had 90 days.

The Gadget Access approach: treat compliance as an operating model

Instead of starting with the annual report form, Gadget Access started with a service continuity question: what must keep working for citizens, customers and dependent sectors, and what would stop it? That shifted workshops from "which control clause do we map to?" to "which service fails, who knows, who decides, and where is the proof?"

Gadget Access' Continuous Compliance framework uses four design rules: scope the real asset, turn controls into evidence, use governance to force decisions, and make the evidence repeatable. The work was split into three sprints.

Days 1 to 30 were about scope and evidence. The team confirmed in-scope assets and owners, built a service-to-component map, identified critical workers and major suppliers, and created a single evidence ledger. This was not a GRC beauty contest. It was a disciplined effort to stop asking the same question five times. Every control owner knew which asset, risk, evidence artefact and decision they were responsible for.

Days 31 to 60 focused on material risk treatment. Workshops were run across cyber and information, personnel, supply chain, and physical and natural hazards. The cyber stream targeted practical controls first: MFA, privileged access, backups, vulnerability SLAs, segmentation evidence, logging quality and incident triage. Procurement reviewed supplier clauses and data processing notifications. Operations validated the uncomfortable edge cases, such as a supplier outage that does not look like a cyber incident at first, but still affects availability.

Days 61 to 90 turned the work into board consumable outputs and an operating rhythm. The Risk Management Program was refreshed, control evidence was linked to owners, an annual report pack was prepared, and the incident reporting playbook was tested through a tabletop exercise. The board did not get a 180-page technical artefact and a prayer. It got a decision pack showing the risk position, treatment plan, residual risk acceptance and evidence that the organisation could keep the program alive after the consultants left.

Figure 1. A 90-day compliance acceleration model that keeps evidence moving after the initial advisory engagement.

Day 90 result snapshot

Area	What changed
Compliance outcome	Board ready Risk Management Program and annual report pack completed inside the 90-day engagement window.
Critical service evidence	Dependency model reached 94 percent coverage for critical services, with evidence mapped to assets, risks and owners.
Identity uplift	Admin and remote access MFA coverage moved from 71 percent to 98 percent.
Exposure management	Critical internet exposed remediation moved from a typical 30-day target to a 14-day executive tracked SLA.
Supplier risk	26 high-risk supplier gaps were either remediated or moved into commercial treatment plans.
Incident readiness	Tabletop reporting decision made in 35 minutes using a rehearsed 12/72-hour decision tree.

Measured uplift without pretending 90 days fixes everything

At day 90, the operator had a board ready Risk Management Program and annual report pack, but the more valuable outcome was decision speed. The asset inventory and dependency model reached 94 percent coverage for critical services. Admin and remote access MFA coverage lifted from 71 percent to 98 percent. The vulnerability process moved critical internet exposed remediation from a typical 30-day target to a 14-day executive tracked SLA, with emergency exceptions reviewed weekly.

Supplier risk reviews were triaged, with 26 high-risk supplier gaps either remediated or moved into commercial treatment plans. Mean time to find compliance evidence fell from hours to under 30 minutes because evidence was tagged to assets, risks and owners.

In the tabletop exercise, the incident reporting decision was made in 35 minutes. That matters. SOCI reporting timeframes are not generous, especially when the first hour of a real incident usually contains confusion, duplicate calls and at least one person asking whether the outage is really cyber. A rehearsed decision tree is worth more than a laminated crisis plan that no one has opened since induction.

Where CiBRAI changed the operating conversation

Traditional SOCI and uplift programs are often smothered by tool-sprawl. A vulnerability scanner knows one truth. EDR knows another. The SIEM sees logs. The SOAR tool sees playbooks. The GRC platform sees policies. Threat intelligence sees the outside world. Procurement sees suppliers. None of them, on its own, can answer the board's simplest question: are we more resilient this month than last month?

This is where CiBRAI becomes more than a cyber dashboard. In a mature model, CiBRAI acts as the cyber operating layer that connects SIEM, SOAR, CTI, case management, reporting and control evidence. Its value is not that it adds yet another pane of glass. Everyone already has enough glass to build a greenhouse. Its value is reducing the distance between telemetry, risk, action and audit.

For the operator, the target state was a living evidence model. A privileged access change, a critical vulnerability, a supplier incident, a failed backup or an anomalous OT network event should not drift around as disconnected signals. It should become context: which critical service is affected, which SOCI hazard vector is implicated, which playbook is triggered, which executive needs to know, and what audit evidence is produced.

CiBRAI's agentic AI approach and support for current on-premise and cloud LLM patterns gives lean teams a path to automate triage and reporting without handing away sovereignty, accountability or common sense.

Figure 2. CiBRAI and Continuous Compliance as an operating layer between telemetry, control evidence and executive reporting.

The future risk: AI compresses the exploit window

The timing of this case is important. AI powered vulnerability discovery is moving from curiosity to strategic pressure. Anthropic's Project Glasswing and Claude Mythos Preview are a strong signal: frontier models are being used to find and

fix software vulnerabilities at speeds that traditional patch governance was not built for. Whether Mythos itself is available to Australian operators is less important than the trend. Offensive and defensive automation are both accelerating.

That changes how SOCI programs should think. The old model says discover, assess, raise ticket, chase owner, report status, repeat until everyone is tired. The new model needs continuous exposure management, automated evidence, faster isolation, integrated threat intelligence and governance that can approve exceptions in hours, not calendar quarters. Compliance frameworks do not make systems safe by existing. They make systems safer when they force timely decisions.

Gadget Access sees this as the next maturity step for Australian critical infrastructure. vCISO advisory, technical uplift and vendor management still matter. So do Essential Eight, ISM, ISO 27001 and NIST mappings. But the winning model is not a bigger spreadsheet. It is a simpler cyber operating system where every control can be tested, every exception has an owner, and every material risk can be explained in plain language to the board.

Lessons for executives

First, SOCI compliance is a service resilience problem, not a paperwork problem. Begin with critical services and dependencies. Second, do not separate compliance from operations. If the evidence only exists the week before an audit, it does not exist in the way you need during an incident. Third, kill tool-sprawl gently but firmly. The goal is not fewer tools for aesthetic reasons. The goal is fewer blind handoffs. Fourth, rehearse reporting decisions. The 12/72-hour clock is not a theoretical construct. It is a management system design test.

Conclusion

The operator did not become magically secure in 90 days. Good security does not work like a kitchen renovation show. What changed was the organisation’s ability to know its obligations, explain its risks, produce evidence and act faster when something moved. That is a very different kind of compliance. It is pragmatic, measurable and operational.

For Gadget Access, this is the point of Continuous Compliance: turn regulatory obligation into a sustainable security capability. For CiBRAI, it is the platform opportunity: give lean cyber teams the operating layer they need to connect alerts, controls, risks and reports before the next incident turns into a board agenda item. SOCI compliance is the starting line. Cyber resilience is the race.

References and source notes

Sources checked on 29 April 2026. This article is general information and is not legal advice.

Cyber and Infrastructure Security Centre: Security of Critical Infrastructure Act 2018

Cyber and Infrastructure Security Centre: Responsible Entity Risk Management Program Annual Report

Cyber and Infrastructure Security Centre: Guidance for the Critical Infrastructure Risk Management Program

Cyber and Infrastructure Security Centre: Notification of Cyber Security Incidents Guidance

Australian Signals Directorate: Annual Cyber Threat Report 2024-2025

Anthropic: Project Glasswing, Securing critical software for the AI era

CiBRAI: CiBRAI Platform and AgentiXCyber