Webinar

vCISO vs. Full-Time CISO: Making the Right Decision for Your Organisation

When a vCISO is the right answer, what to look for, and how to structure the engagement for maximum impact.

By Gadget Access

Header image: cyber leadership decision-making, from board risk to operational evidence.

Webinar brief

A CISO is no longer a person who occasionally reviews firewall projects and writes a security policy in their spare time. The modern CISO is part strategist, translator, incident commander, investment adviser, governance lead and calm adult in the room when a breach, audit, transformation or board question lands without warning. That creates a practical question for many organisations. Do you need a full-time CISO on staff, or do you need the capability, judgement and structure of a vCISO delivered in a more flexible model?

ASD's ACSC reported more than 42,500 calls to the Australian Cyber Security Hotline in FY2024-25, more than 1,200 cyber security incidents responded to, and an average self-reported cybercrime cost per report of $65,000 for small business, $97,200 for medium business and $157,700 for large business. Meanwhile, boards are dealing with Essential Eight uplift, privacy obligations, supply chain risk, cloud security, AI adoption, operational resilience and regulator attention. Security leadership is no longer optional. The question is what form of leadership best fits the organisation's risk, scale and pace.

The real choice is not job title. It is operating model.

The choice between a vCISO and a full-time CISO is not a status symbol. It is an operating model decision. A full-time CISO is right when cyber risk is persistent, complex and material enough that the organisation needs dedicated executive security leadership every day. A vCISO is right when the organisation still needs serious security leadership, but the workload, budget profile, maturity stage or transformation cadence does not justify a permanent executive role.

The trap is confusing presence with impact. A full-time CISO with no authority is expensive theatre. A vCISO with a clear mandate, executive access and a measurable roadmap can be transformational. Conversely, a vCISO who is treated like a part-time compliance note taker will not deliver much beyond document production. Success depends less on whether the person is permanent and more on whether the operating model gives them access, authority, context and evidence.

The decision lens

Diagram 1: The CISO engagement model should follow risk complexity, internal maturity and the level of authority required.

When a vCISO is the right answer

A vCISO is often the right model for small and medium organisations that need board-level cyber judgement without the cost or utilisation problem of a permanent executive. It is also a strong model for organisations with a capable IT team but no senior cyber strategist, and for larger businesses that need an experienced uplift leader while they stabilise governance, rationalise vendors, improve reporting or prepare for a future permanent appointment.

The vCISO model works particularly well during uplift periods. Essential Eight maturity, PSPF alignment, ISM control interpretation, ISO 27001:2022 implementation, NIST CSF 2.0 mapping, incident response improvement, third-party risk reviews and board reporting redesign are all areas where an experienced vCISO can create disproportionate value. These are not just policy exercises. They are translation problems between business priorities, technical debt, vendor claims and risk treatment sequencing.

A vCISO is also useful as an interim leader after a resignation, during a merger, before a regulatory deadline, after an incident, or when an organisation wants to test the shape of the security function before committing to a permanent executive role. In many cases, a vCISO is the fastest route to executive clarity because they arrive without internal baggage and can call out complexity theatre before it becomes next year's budget line.

When a full-time CISO is the right answer

A full-time CISO is usually the better model when the organisation's risk profile demands permanent executive presence. That can include critical infrastructure, regulated data-heavy businesses, large distributed environments, very active acquisition programs, constant incident pressure, or enterprises where security decisions have to be made daily across architecture, identity, cloud, engineering, legal, operations and board stakeholders.

The March 2026 ASD ISM guidance is a useful anchor. It describes the CISO as responsible for overseeing the cyber security programme, coordinating security risk management between cyber and business teams, and ensuring adequate monitoring, reporting and governance. In environments with continuous transformation and high consequence risk, that function can be too embedded and too immediate to treat as a fractional assignment.

The full-time model is not automatically superior. It is superior when it gives the organisation faster decisions, clearer accountability and stronger execution. It is weaker when the CISO becomes a lonely figurehead who owns the risk register but not the budget, delivery teams or technology decisions. If the organisation cannot support the role properly, permanence will not fix the operating model.

What to look for in a vCISO

A good vCISO needs board credibility and technical scar tissue. They must be able to explain risk in financial, operational and legal terms, but they should also understand what happens when a firewall rule, a cloud permission, a legacy identity store or a poorly integrated SOC platform becomes the real source of exposure. A strong vCISO can move from board paper to technical workshop without losing the thread.

Look for Australian framework depth. For many organisations this means Essential Eight, PSPF, ISM, ISO 27001:2022, NIST, SOCI obligations where relevant, privacy obligations and procurement risk. Just as importantly, look for operating experience. A useful vCISO knows how projects stall, how internal politics

distort priorities, how vendors oversell, and how evidence gets lost between tools, spreadsheets and committees.

Vendor independence is another major test. A vCISO must know when a new tool solves a problem and when it simply gives the team another console to feed. Traditional cyber programmes often sprawl across SIEM, SOAR, CTI, EDR, attack surface monitoring, vulnerability scanning, ticketing, GRC, email security, CASB, IAM, PAM and cloud posture tools. That stack can become a museum of overlapping licenses and disconnected dashboards. A serious vCISO should help reduce this sprawl, not add to it.

AI changes the timing problem

Frontier AI is changing vulnerability discovery and defensive operations. Anthropic's Project Glasswing gives selected partners access to Claude Mythos Preview to find and fix vulnerabilities or weaknesses in code. That is a signpost for where the market is heading. Vulnerability research, threat analysis and control validation are moving faster, which increases both the opportunity and the governance challenge.

IBM's 2025 data breach research also points to the governance side of the AI problem, reporting that AI adoption is outpacing security oversight and that 63 percent of organisations lacked AI governance policies despite broad deployment. In practical terms, that means security leaders need to understand both offensive change and defensive opportunity. A vCISO can be particularly useful here because they can help an organisation assess where AI materially improves outcomes and where it simply introduces fresh risk and vendor theatre.

How to structure the engagement for maximum impact

The most successful vCISO engagements start with a charter, not a statement of work full of vague advisory language. The charter should define the reporting line, authority, decision rights, escalation path, meeting cadence, board visibility, priority outcomes and expected artefacts. If the vCISO is responsible for cyber strategy but cannot access business leaders, project owners, managed service providers or evidence sources, the engagement will drift quickly into PowerPoint purgatory.

The first 30 days should establish the truth. That means understanding critical business services, crown-jewel data, current incidents, major suppliers, identity exposure, backup recoverability, logging quality, security architecture debt, regulatory obligations and board expectations. It also means working out where the organisation already has useful controls and where it only has optimistic slideware.

Days 31 to 60 should turn diagnosis into funded action. This is where control owners are assigned, risk treatment is sequenced, vendors are challenged, reporting is simplified and quick wins are separated from longer structural improvements. If the engagement has real teeth, this is also where wasted architecture starts to surface. Duplicate tools, underused platforms and unsupported integrations should all be fair game.

After that, the engagement should settle into an operating rhythm. Weekly delivery sessions keep work moving. Monthly executive reporting keeps risk visible. Quarterly steering committees make decisions on investment, exceptions and major dependencies. The vCISO should not become a distant adviser who sends a PDF once a month. They should become a working part of the leadership system.

Where Gadget Access and CiBRAI fit

Diagram 2: A vCISO engagement works best when governance, control ownership, tool evidence and reporting cadence are designed together.

Gadget Access approaches vCISO work from three decades of IT, infrastructure, networking, cyber operations and vendor management experience. That matters because vCISO advice has to survive contact with reality. It has to account for legacy platforms, procurement friction, budget pressure, integration headaches and the very human tendency for organisations to buy one more tool rather than fix the operating model.

Our trademarked Continuous Compliance framework is designed for exactly this gap between strategy and evidence. It keeps controls, risks, exceptions, remediation actions and reporting alive as a managed operating rhythm rather than a once-a-year compliance event. For boards and executives, that means clearer visibility. For delivery teams, it means less ambiguity and more practical sequencing.

CiBRAI strengthens this operating model by giving teams a unified signal view across endpoint, cloud, identity and network, supported by agentic AI that groups events, adds context and prioritises action. That matters in the vCISO conversation because leadership quality is often undermined by fragmented evidence. When the data is spread across too many disconnected tools, strategy becomes guesswork. A more unified cyber operating system gives both the vCISO and the internal team a stronger platform for faster decisions and leaner architecture.

AI will not chair your risk committee. It can, however, stop the committee arguing over which spreadsheet is the real one. That is where the combination of vCISO leadership, Continuous Compliance and CiBRAI becomes strategically interesting.

The final decision

The right question is not, can we afford a CISO? The better question is, what cyber leadership does our risk require, and how quickly do we need it to operate? A vCISO can be the right answer when the organisation needs high-value judgement, structure and uplift without unnecessary executive overhead. A full-time CISO is the right answer when the risk and decision load justify a permanently embedded leader with broad internal reach.

The strongest answer is often hybrid. Use a vCISO to establish governance, uplift controls, rationalise vendors and build board confidence, then decide whether to retain the model, appoint a full-time leader, or combine both during a transition. Either way, make the decision based on risk, complexity and execution needs, not prestige. Cyber security has enough vanity architecture already.

What the webinar will unpack

The webinar will examine where a vCISO creates faster value, when a full-time CISO is justified, what capabilities and leadership traits to look for, and how to structure an engagement model that improves governance, reporting, delivery and measurable cyber outcomes.

Selected references

These sources were used to ground the article in current Australian cyber guidance, workforce data, breach statistics, AI security developments and the CiBRAI platform context.

Australian Signals Directorate, ACSC. Annual Cyber Threat Report 2024-25. Link

Australian Signals Directorate. Using the Information Security Manual, March 2026. Link

Australian Signals Directorate. ISM Guidelines for Cyber Security Roles, March 2026. Link

Australian Signals Directorate. The Commonwealth Cyber Security Posture in 2025. Link

Office of the Australian Information Commissioner. Latest Notifiable Data Breach statistics for January to June 2025. Link

ISACA. State of Cybersecurity 2025 global press release. Link

IBM. Cost of a Data Breach Report 2025. Link

NIST. Cybersecurity Framework 2.0. Link

Anthropic. Project Glasswing: Securing critical software for the AI era. Link

CiBRAI. Unified Cyber Security Platform with AI. Link

CiBRAI. AI-Integrated Threat Intelligence Platform. Link

Prepared for Gadget Access Resources. Updated article images enhanced for this document.