CISO Advisory
AUSTRALIA

CAPABILITY STATEMENT

Independent Cyber Security Leadership

Independent Cyber Security Advisory & Virtual CISO services for Australian government, councils, regulated entities and enterprise.

Senior, vendor-neutral security leadership and assurance on demand — assessed against the frameworks your obligations actually require, and reported in language your board can act on.

cisoadvisory.com.au · 07 2112 8502
Australia-wide · On-site or remote · 24/7

A Digital One Agency company
Capability Statement · June 2026

EXECUTIVE OVERVIEW

Senior Cyber Security Leadership, On Demand

CISO Advisory Australia provides independent, vendor-neutral cyber security advisory and Virtual CISO services to Australian government, councils, regulated entities and enterprise. We deliver the judgement, assurance and board-level accountability of a senior Chief Information Security Officer — without the cost, recruitment risk or commitment of a full-time executive hire.

Most Australian organisations now face the same uncomfortable equation. The regulatory and threat environment demands executive-grade security leadership: directors are personally accountable for cyber resilience, regulators expect demonstrable governance, and procurement panels increasingly require evidence of maturity against named frameworks. Yet experienced security executives are scarce, expensive, and difficult to retain — and for most organisations under a certain scale, a full-time CISO is neither affordable nor necessary.

CISO Advisory exists to close that gap. We provide senior security leadership and independent assurance as a service: assessing where you genuinely stand, building the governance and control environment your obligations require, reporting to your board in language directors can act on, and standing behind our findings when an auditor, regulator or acquirer asks how you know what you claim to know.

Independent by design

We are advisers and assessors only. We do not resell security products, take referral commissions, or hold reseller agreements with any vendor. When we recommend a control, a tool or an architecture, the recommendation is driven solely by your risk profile, your obligations and your budget — never by a margin. In a market where much "advice" is a sales channel in disguise, that independence is the foundation of everything we produce: findings you can defend, roadmaps you can trust, and reports that survive scrutiny.

Senior-led, every engagement

Every engagement is led by our Founder & Principal Advisor, Ken Armitt, who brings 27 years of hands-on experience across cyber security, SaaS, fintech, payments and government-facing systems. The person who scopes your engagement is the person who does the work and presents to your board. You will not be handed off to a junior bench after the proposal is signed.

27	100%	Senior-led	24/7
years hands-on experience	independent & vendor-neutral	every engagement, end to end	Australia-wide, on-site or remote

CISO Advisory Australia is a Digital One Agency company, serving clients Australia-wide — on-site same day or next business day, or fully remote, around the clock.

CONTEXT

The Environment You Operate In

Australian organisations are governed by one of the most demanding cyber regulatory environments in the world — and it is tightening every year. Understanding what is actually required of you, and what regulators and courts now expect of directors, is the starting point for any credible security program.

Directors are personally accountable

Cyber security is no longer an IT line item; it is a directors' duty. ASIC has made clear that it regards cyber resilience as a core governance responsibility and has pursued enforcement action against licensees whose risk management of cyber threats was found inadequate. APRA has been equally direct with the entities it regulates. The practical consequence: a board that cannot demonstrate informed, active oversight of cyber risk — with evidence, not assurances — carries personal and organisational exposure. "We relied on IT" is not a defence available to a modern Australian board.

The Essential Eight is becoming the de facto national baseline

The ACSC's Essential Eight, embedded in the Protective Security Policy Framework, is effectively mandatory across federal non-corporate Commonwealth entities and is increasingly expected of state agencies, local councils, and any supplier seeking government work. Tender questionnaires now routinely ask for a stated maturity level — and increasingly for evidence behind it. Organisations that self-assess optimistically discover the gap at the worst possible moment: during an audit, a procurement evaluation, or an incident post-mortem.

APRA-regulated entities: CPS 234 and the shift to CPS 230

Entities regulated by APRA must meet CPS 234 (Information Security), which imposes explicit obligations on information security capability, control testing, third-party assurance and incident notification. APRA's CPS 230 (Operational Risk Management) goes further, requiring regulated entities to manage operational risk — including technology and cyber risk — as an integrated discipline, with demonstrable resilience of critical operations and far deeper accountability for material service providers. The combined effect is that information security can no longer be assessed in isolation from operational resilience, and board reporting must connect the two.

Critical infrastructure: the SOCI Act

The Security of Critical Infrastructure (SOCI) Act imposes binding obligations on operators of critical infrastructure assets across an expanded range of sectors — including risk management programs covering cyber, physical, personnel and supply-chain hazards, mandatory cyber incident reporting on short statutory timeframes, and enhanced obligations for the most significant systems. Many organisations captured by the expanded definitions are still coming to terms with the fact that they are now regulated critical infrastructure operators.

Privacy reform is raising the cost of failure

The Privacy Act 1988 and the Notifiable Data Breaches scheme already require organisations to assess and notify eligible data breaches. The ongoing program of Privacy Act reform has sharply increased maximum penalties for serious or repeated interferences with privacy, strengthened the regulator's enforcement powers, and introduced new avenues of liability — raising the standard of accountability expected when personal information is mishandled. Data governance and breach readiness are now board matters, not back-office hygiene.

Standards have moved — and so has the threat

ISO/IEC 27001 transitioned to its 2022 revision, restructuring the control set and adding controls for cloud security, threat intelligence and data leakage prevention; certifications now operate against the 2022 standard. NIST released CSF 2.0, elevating governance to a function in its own right. Meanwhile the ACSC continues to report a relentless volume of incidents against Australian organisations of every size, with business email compromise, ransomware and identity-based attacks doing the most damage — and social engineering remaining the most reliably successful attack vector against otherwise well-defended organisations.

> **Why this points to independent senior advisory**
>
> Every one of these obligations ultimately asks the same question: *can you demonstrate, with evidence, that your security posture matches your obligations and your risk?* Answering that question requires senior expertise that most organisations cannot justify employing full-time — and independence that an organisation selling you products can never credibly offer. That is precisely the gap CISO Advisory fills.

CAPABILITIES

Core Capabilities — At a Glance

Twelve capabilities, one consistent discipline: evidence-based assessment, prioritised by real risk, reported in language a board can act on. Each capability is detailed in the pages that follow.

Capability	Outcome it delivers	Primary frameworks
Virtual CISO (vCISO) & security leadership	Executive-grade security leadership, governance and accountability without a full-time hire	All — tailored to your obligations
Cyber risk assessment & security governance	A defensible, board-level view of cyber risk and a governance structure that satisfies directors' duties	NIST CSF 2.0, ISO 27001, ISM
Essential Eight assessment & uplift	An evidence-based maturity rating (ML1–ML3) and a sequenced uplift roadmap	Essential Eight, ISM, PSPF
ISO/IEC 27001:2022 readiness & certification support	An ISMS built for certification and genuine operation — not shelf-ware	ISO/IEC 27001:2022
APRA CPS 234 & CPS 230 compliance	Demonstrable compliance with APRA's information security and operational risk standards	CPS 234, CPS 230
ISM / PSPF alignment & IRAP readiness	Government-grade security posture and confident preparation for IRAP assessment	ISM, PSPF, IRAP (readiness)
NIST CSF 2.0 & SOC 2 advisory	Internationally recognised posture for global customers, partners and investors	NIST CSF 2.0, SOC 2
Penetration testing & technical assurance	Verified, exploitable findings across web, network, cloud and people — not scanner output	ISM, PCI DSS, CPS 234, Essential Eight
Independent cyber & IT audits	An objective, evidence-based audit of your environment — on-site, cloud or remote	ISO 27001, ISM, NIST CSF
Cyber due diligence (M&A, pre-IPO, vendor risk)	Cyber risk quantified and surfaced before it prices, delays or derails a transaction	NIST CSF, ISO 27001, SOC 2
AI governance & secure AI adoption	The productivity of AI without uncontrolled data, privacy and security exposure	ISO 27001, Privacy Act, NIST CSF
Incident readiness & response advisory	A tested, board-aware response capability before — and beside you during — an incident	ISM, NDB scheme, SOCI Act, CPS 234

CAPABILITY DEEP-DIVE — LEADERSHIP & GOVERNANCE

Security Leadership & Governance

Virtual CISO (vCISO) & Security Leadership

A Virtual CISO gives you a senior security executive — accountable, available and embedded in your leadership rhythm — at a fraction of the cost of a full-time appointment. This is not a helpdesk or a compliance checkbox: it is genuine security leadership. Your vCISO owns the security strategy, chairs the security agenda with executives, manages the program of work, holds vendors and internal teams to account, and fronts your board, your auditors and your regulators when security is on the table.

- Security strategy and multi-year roadmap aligned to your obligations and risk appetite
- Standing executive and board reporting, including a maintained cyber risk register
- Policy framework ownership: development, review cycles and exception management
- Oversight of internal IT teams, managed service providers and security vendors
- Regulator, auditor and customer security questionnaire representation
- Security input into major decisions — cloud migrations, new products, restructures, acquisitions

Outcome — a named, senior, accountable security leader your board can question and your organisation can rely on, scaled to the size of your actual need.

Cyber Risk Assessment & Security Governance

Directors cannot oversee a risk they cannot see. We translate your technical environment into a structured cyber risk picture: what threatens you, what it would cost, how likely it is, what controls stand in the way, and where the genuine gaps are. We then build the governance machinery — risk appetite statements, reporting cadence, ownership and escalation — that turns that picture into ongoing board oversight rather than a one-off snapshot. Everything is framed so a non-technical director can interrogate it, because that is precisely what regulators now expect directors to be able to do.

- Threat and risk assessment grounded in your actual systems, data and dependencies
- Cyber risk register with likelihood, impact, control effectiveness and risk ownership
- Risk appetite and tolerance statements suitable for board adoption
- Board reporting framework: metrics, cadence and escalation thresholds that directors can defend
- Security governance structure — committees, roles, and accountability mapping

Outcome — a cyber risk position your board can state, evidence and defend — to a regulator, an insurer, an acquirer or a court.

Independent Cyber & IT Audits

An audit is only as valuable as the independence of the auditor. Because we sell no products and carry no vendor allegiance, our audits report what we find — not what a sales pipeline needs us to find. We audit on-site, in cloud environments, and fully remotely: configuration against hardening baselines, identity and access against least privilege, backup and recovery against tested reality, vendor arrangements against contract, and claimed controls against operating evidence. Where your obligations specify a framework, we audit against that framework explicitly.

- On-site audits of infrastructure, networks, physical controls and operational practice
- Cloud security audits across major platforms — identity, configuration, segmentation, logging
- Off-site/remote audits for distributed organisations and time-sensitive reviews
- Evidence-based testing of claimed controls — we verify, we do not accept attestations at face value
- Findings register with severity, root cause and pragmatic remediation for every item

Outcome — an objective account of how your environment actually operates, signed by an assessor with no incentive to soften or inflate it.

CAPABILITY DEEP-DIVE — AUSTRALIAN FRAMEWORKS

Australian Government & Regulatory Frameworks

Essential Eight Assessment & Uplift — Maturity Level 1 to 3

The ACSC Essential Eight is the baseline the Australian Government measures itself against, and the bar councils, agencies and suppliers are increasingly held to. We assess your true maturity across all eight mitigation strategies — application control, patch applications, configure Microsoft Office macro settings, user application hardening, restrict administrative privileges, patch operating systems, multi-factor authentication, and regular backups — and we separate what is claimed from what is evidenced. Most organisations that self-assess at ML2 are not at ML2; we tell you where you genuinely sit and exactly why.

- Evidence-based maturity assessment against ML1, ML2 and ML3 using ACSC assessment guidance
- Gap analysis identifying the specific control failures behind each maturity shortfall
- A prioritised uplift roadmap sequenced by risk reduction and implementation effort
- Re-assessment after remediation, so the rating you report is one you can stand behind

Outcome — a defensible maturity rating you can show an auditor, a regulator, a tender panel or a board — and a clear, costed path to the level your obligations require.

ISM / PSPF Alignment & IRAP Readiness

Organisations that hold, process or aspire to handle Australian Government information must align with the ACSC Information Security Manual and the Protective Security Policy Framework — and, for many systems, face IRAP assessment. We help you get there with eyes open: mapping the ISM controls applicable to your system's classification, building the system security documentation an assessor will expect, closing control gaps before they become findings, and preparing your team for the assessment itself. We prepare you for IRAP assessment; we are candid that the formal assessment is conducted by an endorsed IRAP assessor, and we help you engage and get full value from that process.

- ISM control applicability mapping and gap assessment for your system and classification level
- PSPF alignment across governance, information, personnel and physical security domains
- System security plans, risk assessments and supporting artefacts built to assessor expectations
- Remediation program management and pre-assessment readiness review

Outcome — you walk into IRAP assessment — or a government security review — prepared, documented and without surprises.

APRA CPS 234 & CPS 230 Compliance

APRA-regulated entities carry two interlocking obligations: CPS 234's explicit requirements for information security capability, control testing and incident notification, and CPS 230's broader demand that operational risk — including technology, cyber and material service providers — be managed as a single, board-owned discipline with demonstrably resilient critical operations. We assess your current position against both standards, close the gaps, and build the ongoing testing and assurance rhythm APRA expects to see operating — not merely documented.

- CPS 234 gap assessment: capability, policy framework, control testing, third-party assurance, notification readiness
- CPS 230 alignment: critical operations mapping, tolerance levels, service provider management
- Information security control testing programs with evidence trails fit for APRA review
- Board and senior management reporting that connects information security to operational resilience

Outcome — a compliance position you can evidence to APRA, integrated rather than bolted on, and maintained through a sustainable assurance cycle.

CAPABILITY DEEP-DIVE — INTERNATIONAL STANDARDS & ASSURANCE

Certification, Standards & Technical Assurance

ISO/IEC 27001:2022 Readiness & Certification Support

ISO/IEC 27001 remains the most widely recognised signal that an organisation manages information security systematically — and since the 2022 revision, with its restructured Annex A and new controls for cloud security, threat intelligence and data leakage prevention, certification requires more than re-badging old documents. We build information security management systems designed to pass certification audit *and* to be genuinely operated afterwards. An ISMS that exists only in a document repository fails its first surveillance audit and protects nothing; we build the lighter-weight, operationally honest version that survives both.

- Gap assessment against ISO/IEC 27001:2022 including the revised Annex A control set
- ISMS design: scope, risk methodology, Statement of Applicability, policy suite
- Control implementation support and internal audit ahead of certification
- Certification body liaison and support through Stage 1 and Stage 2 audits
- Post-certification operating rhythm: management review, internal audit, continual improvement

Outcome — certification you can win, keep and honestly stand behind — with an ISMS sized for your organisation, not a template's.

NIST CSF 2.0 & SOC 2 Advisory

Organisations selling into North American markets, raising international capital, or serving enterprise customers are increasingly asked for posture against NIST CSF and SOC 2. NIST CSF 2.0's elevation of governance to a first-class function mirrors where Australian regulation is heading, which makes it an excellent organising framework even for purely domestic organisations. We assess and build against CSF 2.0, and we prepare organisations for SOC 2 examination — designing the control environment, evidence collection and operational discipline that a Type II report demands across a live audit period.

- NIST CSF 2.0 maturity assessment across Govern, Identify, Protect, Detect, Respond and Recover
- Target-state profiling and roadmap aligned to business strategy and customer expectations
- SOC 2 readiness: Trust Services Criteria scoping, control design, evidence automation
- Audit-period support and auditor liaison through Type I and Type II examinations

Outcome — internationally legible security posture that opens doors with enterprise customers, partners and investors.

Penetration Testing & Technical Assurance

Frameworks tell you what should be true; penetration testing tells you what is. We conduct controlled, authorised attacks against your web applications, networks and infrastructure, cloud environments, and — critically — your people. Social engineering is where most organisations are weakest: a workforce that has never been tested against a competent phishing or pretexting campaign is an unlocked door behind an expensive fence. Our findings are verified and exploitable, ranked by genuine business impact, and explained in terms an executive can act on — not raw scanner output rebadged as a report.

- Web application testing: authentication, authorisation, injection, session and business-logic flaws
- Network and infrastructure testing, external and internal, including lateral-movement analysis
- Cloud security testing: identity, misconfiguration, exposed services and privilege escalation paths
- Social engineering: phishing campaigns, pretexting and physical/personnel testing by agreement
- Retesting after remediation, with an attestation letter confirming closure

Outcome — proof of where you are actually exploitable, what it would have cost you, and evidence of closure once it is fixed.

CAPABILITY DEEP-DIVE — TRANSACTIONS, AI & INCIDENTS

Due Diligence, AI Governance & Incident Readiness

Cyber Due Diligence — M&A, Pre-IPO & Vendor Risk

Cyber risk is transaction risk. An undisclosed breach, an indefensible security posture or a non-compliant data practice discovered late can reprice a deal, delay a listing or surface as a warranty claim years later. We conduct cyber due diligence for acquirers assessing targets, for vendors preparing to be assessed, and for boards preparing companies for IPO — where prospectus-grade scrutiny of risk disclosure leaves no room for optimistic self-assessment. The same discipline applies to ongoing third-party and vendor risk: the suppliers inside your trust boundary are part of your attack surface, and regulators from APRA to the SOCI regime now expect you to manage them as such.

- Acquirer-side due diligence: posture assessment, breach-history indicators, integration risk
- Sell-side and pre-IPO readiness: finding and fixing issues before the other side's advisers do
- Third-party / vendor risk programs: tiering, assessment, contractual controls, ongoing monitoring
- Clear, quantified reporting suitable for deal teams, boards and disclosure processes

Outcome — cyber risk surfaced, quantified and priced before it can damage the transaction — or your reputation after it.

AI Governance & Secure AI Adoption

AI adoption is happening in your organisation whether you have sanctioned it or not. Staff are pasting commercial information into public tools; teams are wiring AI into products and workflows; vendors are embedding it into platforms you already use. The risk is not AI itself — it is ungoverned AI: data leakage, privacy breaches, unreliable outputs in consequential decisions, and obligations under the Privacy Act that do not pause because the processing happened in a model. We help boards and executives capture AI's productivity honestly: a governance framework that says what is permitted, with what data, under whose accountability — and the security controls that make the policy real.

- AI usage discovery: what is actually in use across the organisation, sanctioned and shadow
- AI governance framework: acceptable use, data classification rules, approval and accountability
- Security and privacy assessment of AI tools, vendors and integrations before adoption
- Secure-by-design guidance for AI features in your own products and services
- Board education on AI risk, opportunity and the emerging regulatory direction

Outcome — AI adopted deliberately and defensibly — with the upside captured and the data, privacy and reputational exposure controlled.

Incident Readiness & Response Advisory

The cost of a cyber incident is largely determined before it happens — by whether a tested plan exists, whether roles are clear, and whether the board knows its obligations under the Notifiable Data Breaches scheme, the SOCI Act's reporting timeframes, CPS 234 notification requirements and continuous disclosure rules where they apply. We build and test that readiness in calm conditions, and we sit beside your executives during a live incident as an independent adviser: helping you make defensible decisions under pressure, coordinate specialist responders, and manage regulators, insurers, customers and the record that will be examined afterwards.

- Incident response plans and playbooks for your most plausible scenarios
- Executive and board tabletop exercises — tested under realistic pressure, gaps captured and fixed
- Regulatory notification mapping: who must be told, of what, and within what timeframe
- Live-incident executive advisory: decision support, coordination and regulator engagement
- Post-incident review: root cause, lessons, and the remediation evidence regulators expect

Outcome — when the worst day comes, your organisation responds in hours with a rehearsed plan — not in days with an improvised one.

METHOD

How We Work — The Engagement Lifecycle

Every engagement follows the same disciplined lifecycle, whether it is a two-week assessment or a multi-year retained relationship. The structure exists for one reason: so that what we find is evidenced, what we recommend is prioritised, and what we report is defensible.

1. **Discovery call**
   A focused conversation about your obligations, your environment and what is driving the engagement — at no cost and no obligation.

2. **Scope & agree**
   A written scope with clear boundaries, deliverables, timeframes and a fixed or clearly structured fee. No open-ended billing, no scope surprises.

3. **Assess & test**
   Evidence-based assessment and, where in scope, authorised technical testing. We verify claims against operating reality — interviews alone are not evidence.

4. **Board-ready reporting**
   Findings delivered twice: an executive narrative your board can act on, and a technical register your teams can implement from. Presented in person where wanted.

5. **Remediate & retest**
   Prioritised remediation support, then re-assessment of closed items — so your final position is verified, not assumed.

Cadence to match the need

Some organisations need a single, decisive assessment — before a tender, a transaction, an audit or a board decision. Others need a quarterly assurance rhythm: posture re-checked, the risk register refreshed, the board pack updated, and the uplift program held to account. Others again need continuous senior leadership through a retained Virtual CISO arrangement, with a standing presence in executive forums and an agreed monthly commitment. We operate all three cadences, and engagements move between them as your needs change — a one-off assessment frequently matures into a quarterly program once a board has seen what informed oversight looks like.

DELIVERABLES

What You Receive

Every deliverable we produce is built to two standards: a director must be able to act on it without translation, and an auditor or regulator must be able to rely on it without caveat. We do not produce shelf-ware — documents that exist to be filed rather than used waste your money and protect nothing.

Executive risk summary

A concise, plain-English account of your security position: the risks that matter, what they would cost, and the decisions required — written for directors and executives, not technologists.

Framework gap assessment with maturity scoring

Your position against each in-scope framework — Essential Eight, ISO 27001:2022, CPS 234/230, ISM, NIST CSF 2.0 — scored control by control, with the evidence behind every rating.

Prioritised remediation roadmap

Every gap sequenced by risk reduction, effort and dependency — so your teams and budget attack the items that matter first, with realistic timeframes attached.

Board pack

A presentation-ready board paper: posture, trend, top risks, regulatory position and decisions sought. Designed to be minuted — the evidence of oversight that directors' duties now demand.

Technical findings register

The full detail behind the executive narrative: every finding with severity, affected assets, root cause, reproduction evidence and specific remediation guidance.

Attestation & retest letter

Following remediation and retest, formal written confirmation of what was tested, what was found and what is verified closed — suitable for tenders, customers, insurers and auditors.

Policy & standards set

Security policies, standards and procedures written for your organisation's actual size and operations — short enough to be read, specific enough to be followed, mapped to your frameworks.

Cyber risk register & reporting framework

A living risk register with ownership and treatment status, plus the metrics and reporting cadence that keep it alive between engagements rather than decaying in a drawer.

Where an engagement includes incident readiness, deliverables extend to response plans, playbooks, notification matrices and tabletop exercise reports. Where it includes due diligence, reporting is structured for deal teams and disclosure processes. In every case, you own the work product outright.

SECTORS

Sectors We Serve

Our work concentrates where the obligations are heaviest and the cost of getting security wrong is highest. Each sector below carries a distinct regulatory posture — and we advise against the obligations that actually apply to you, not a generic checklist.

Government & local councils

Agencies and councils face Essential Eight expectations, PSPF and ISM obligations, constrained budgets and intense public accountability when incidents occur. We deliver maturity assessments, uplift roadmaps and vCISO leadership scaled to public-sector procurement and governance realities.

Financial services & APRA-regulated entities

Banks, insurers, superannuation trustees and other regulated entities must evidence CPS 234 compliance and operate under CPS 230's integrated operational risk regime. We build the control testing, third-party assurance and board reporting that withstand APRA scrutiny.

Critical infrastructure (SOCI)

Operators captured by the SOCI Act carry risk management program obligations and statutory incident reporting timeframes measured in hours. We help operators build compliant risk management programs and the reporting readiness those timeframes demand.

Healthcare

Health organisations hold the most sensitive personal information Australians have, remain a persistent target for ransomware, and consistently feature among the most-breached sectors under the NDB scheme. We balance clinical continuity, privacy obligations and practical control uplift.

ASX-listed companies

Listed boards face continuous disclosure considerations around material cyber incidents, investor scrutiny of cyber governance, and ASIC's clear expectations of directors. We give boards the independent assessment and reporting that demonstrates informed oversight.

Pre-IPO & IPO-bound companies

A listing exposes your security posture to prospectus-grade scrutiny — from advisers, underwriters and, after listing, regulators and investors. We find and fix the issues before due diligence does, and build the governance story the process expects.

Established private companies ($25M+ turnover)

Substantial private companies carry enterprise-grade cyber risk — customer data, payment flows, supply-chain dependencies, ransomware exposure — without enterprise security budgets. The vCISO model exists precisely for this segment: senior leadership at sustainable cost.

DIFFERENTIATION

Why CISO Advisory

Cyber advisory is a crowded market. These are the specific, structural reasons organisations choose us — and the standards we hold ourselves to on every engagement.

Independent and vendor-neutral — structurally, not rhetorically

We do not resell products, hold reseller margins or accept referral commissions, so no recommendation we make can be motivated by anything other than your interest. This is not a marketing position; it is a business-model decision that makes our findings defensible in front of an auditor, a regulator or a court. Advice from a firm that profits from the remediation it recommends is, by construction, conflicted — ours is not.

Senior expertise on demand

Every engagement is led end-to-end by our Founder & Principal Advisor, with 27 years of hands-on experience across cyber security, SaaS, fintech, payments and government-facing systems. There is no leverage model and no junior bench: the person who wins your trust in the first meeting is the person doing the assessment, writing the report and presenting to your board.

Board-ready communication

Technical findings that directors cannot act on are wasted findings. Everything we produce is written twice — an executive narrative in plain English, and a technical register for implementers — because cyber governance fails most often at the translation layer between the two. We present in the boardroom, take directors' questions directly, and frame risk in the language of duty, cost and decision.

Practical, prioritised outcomes

We will never hand you a 200-item findings list and wish you luck. Every recommendation is sequenced by genuine risk reduction against effort and cost, scoped to your real budget and team, and tracked through to verified closure. The measure of our work is not the thickness of the report — it is the measurable reduction in your exposure six months later.

Compliance aligned to real obligations

We start from the obligations that actually bind you — Essential Eight expectations, CPS 234/230, the SOCI Act, the Privacy Act, contractual security clauses — and build a single control environment that satisfies them together. Organisations that chase frameworks one at a time pay for the same controls three times; we map once and reuse everywhere.

Rapid, Australia-wide response

We serve clients across Australia, on-site same day or next business day, or fully remote — and we are reachable 24/7, because incidents and board deadlines do not keep business hours. Engagements can begin within days of scoping, not after a quarter on a consulting firm's waiting list.

COMMERCIAL

Engagement & Commercial Models

Three engagement models cover the full range of need — from a single decisive assessment to standing executive leadership. All three are scoped in writing, priced transparently before work begins, and free of the structural conflicts that distort much of the market's advice.

Retained Virtual CISO

An ongoing arrangement providing a named senior security leader with an agreed monthly commitment: standing participation in executive and board forums, ownership of the security program, vendor and team oversight, and availability when issues arise. Retainers are sized to your organisation's scale and obligations, reviewed periodically, and adjusted as your maturity grows — the goal is the right amount of leadership, not the largest possible invoice.

Fixed-scope projects

Defined pieces of work with a clear boundary, deliverable set and fee agreed before commencement: an Essential Eight maturity assessment, an ISO 27001:2022 readiness program, a penetration test, a due-diligence review, an incident readiness build. Fixed scope means fixed accountability — you know precisely what you will receive, when, and at what cost.

Ongoing assurance programs

A scheduled rhythm of independent assurance — typically quarterly — combining re-assessment, control testing, risk register maintenance and refreshed board reporting. This model suits organisations that have completed an uplift and need their posture independently verified and kept current, including for regulators, insurers, customers and tender responses.

How engagements are scoped and priced

Pricing follows scope, and scope follows a genuine understanding of your environment — which is why every engagement begins with a discovery conversation at no cost. We quote in plain terms against defined deliverables. Because we sell no products, our fees are our entire commercial interest in the engagement: there is no downstream margin, no remediation pipeline we are incentivised to inflate, and no reason for our findings to be anything other than accurate.

> **How to start**
>
> Book a discovery call on 07 2112 8502 or email contact@cisoadvisory.com.au. Within that conversation we will tell you candidly whether and how we can help; within days you will have a written scope, fixed deliverables and a start date. No cost, no obligation, and no sales process — just a senior practitioner on the other end of the line.

LEADERSHIP

Leadership

CISO Advisory is built on a simple conviction: organisations deserve security advice from someone who has actually built, secured and operated the kinds of systems they run — and who will stake their own name on the findings.

Ken Armitt

FOUNDER & PRINCIPAL ADVISOR

Ken brings 27 years of hands-on experience across cyber security, SaaS platforms, fintech, payments and government-facing systems. His career has spanned the full breadth of the discipline — designing and securing production systems that handle sensitive data and money, assessing environments against Australian and international frameworks, and advising executives and boards on the decisions that security ultimately comes down to: what to protect, what to spend, and what risk to accept.

That combination — deep technical fluency and board-level communication — defines how CISO Advisory operates. Ken personally leads every engagement: scoping it, performing or directly supervising the assessment work, writing the findings, and presenting them to executives and directors. Clients deal with a practitioner who can read a firewall ruleset in the morning and brief a board in the afternoon, and who answers for the quality of the work in person.

Ken founded CISO Advisory Australia, a Digital One Agency company, to give Australian organisations access to that calibre of security leadership without the cost or commitment of a full-time executive — delivered independently, without a product to sell or a vendor allegiance to serve.

GOVERNANCE

Independence, Ethics & Governance

Advisory work is only worth what its independence is worth. These are the commitments under which every CISO Advisory engagement is conducted — without exception, and in writing where you require it.

Vendor neutrality

We hold no reseller agreements, accept no referral fees or commissions, and take no payment from any party other than our client. Where a recommendation involves a product category, we assess options on merit against your requirements and say so plainly — including when the right answer is a capability you already own and are under-using.

Confidentiality

Engagement materials, findings and client identities are held in strict confidence. Security findings are among the most sensitive documents an organisation possesses — a findings register is, in the wrong hands, an attack plan — and we handle them accordingly: access-controlled, shared only with named recipients you authorise, and retained or destroyed according to the terms we agree with you.

Objectivity

We report what the evidence supports — no more and no less. We do not soften findings to preserve relationships, and we do not inflate them to sell remediation work. Where we are uncertain, we say so and state what further evidence would resolve it. A rating from CISO Advisory means the same thing on every engagement, which is precisely what makes it useful to your auditors, your regulators and your board.

Responsible disclosure and lawful conduct

All technical testing is performed under explicit written authorisation, within agreed scope and rules of engagement. Vulnerabilities discovered in third-party products in the course of our work are handled through responsible disclosure to the affected vendor. We operate within Australian law in all engagements and decline work that would require otherwise.

> ***Our only product is the truth about your security posture — delivered early enough, and clearly enough, for you to act on it.***

SUMMARY & CONTACT

Capability Summary & Contact

The essentials for procurement, panel and engagement purposes are set out below. We are pleased to provide any further documentation your process requires.

Item	Detail
Trading name	CISO Advisory Australia
Legal entity	Digital One Agency — CISO Advisory Australia is a Digital One Agency company
ABN	82 307 630 720
Registered address	1 Farrer Place, Sydney NSW 2000
Insurances	Public Liability $39M · Professional Indemnity $30M · Workers' Compensation maintained as required by law. Certificates of currency available on request.
Founder & Principal Advisor	Ken Armitt — 27 years hands-on across cyber security, SaaS, fintech, payments and government-facing systems
Service area	Australia-wide — on-site (same day / next business day) or remote
Availability	24/7
Frameworks & standards	Essential Eight (ML1–ML3) · ISO/IEC 27001:2022 · APRA CPS 234 & CPS 230 · ACSC ISM · PSPF · IRAP readiness · NIST CSF 2.0 · SOC 2 · PCI DSS · Privacy Act 1988 / NDB scheme · SOCI Act
Core services	Virtual CISO · risk assessment & governance · framework assessment & uplift · penetration testing & technical assurance · independent audits · cyber due diligence · AI governance · incident readiness & response advisory
Phone	07 2112 8502
Email	contact@cisoadvisory.com.au
Web	cisoadvisory.com.au

Next step

If your organisation needs to know where it genuinely stands — before a regulator, an auditor, an acquirer or an incident decides to tell you — the next step is a discovery call. Thirty minutes with a senior practitioner, at no cost and no obligation, and you will leave the call knowing whether we can help, how we would scope it, and what it would involve.

Call 07 2112 8502, email contact@cisoadvisory.com.au, or visit cisoadvisory.com.au. We answer 24/7, Australia-wide.