Closing the cyber security execution gap:

How IT leaders are building cyber resilience

Introduction: Australia's cyber threat environment

Australia's cyber threat environment continues to intensify for organisations across the country. The Australian Signals Directorate's (ASD) Annual Cyber Threat Report 2024-25 demonstrates a sustained rise in both threat volume and operational impact.

Together, these trends show that cyber incidents are not only becoming more frequent, but more disruptive and costly to manage.

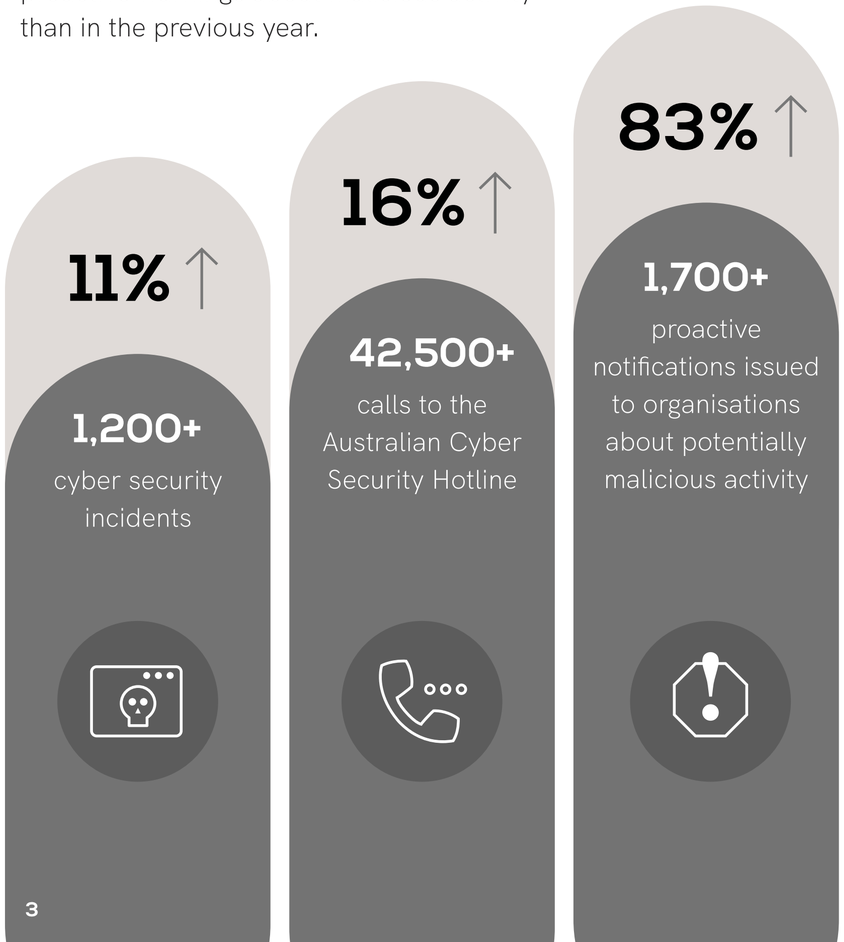
This guide is designed to help mid-market IT leaders move from awareness to action. It outlines how to reduce operational cyber risk, sustain Essential Eight controls in practice, and produce evidence that stands up to boards, regulators, and insurers. The focus is not on new tools, but on running security controls reliably, efficiently, and defensibly in day-to-day operations.

It also recognises that emerging technologies such as AI introduce both benefits and new exposure. As organisations adopt AI across business functions, strong security foundations and clear governance become essential to ensure data is protected, access is controlled, and risk is managed proactively rather than amplified.

Contents

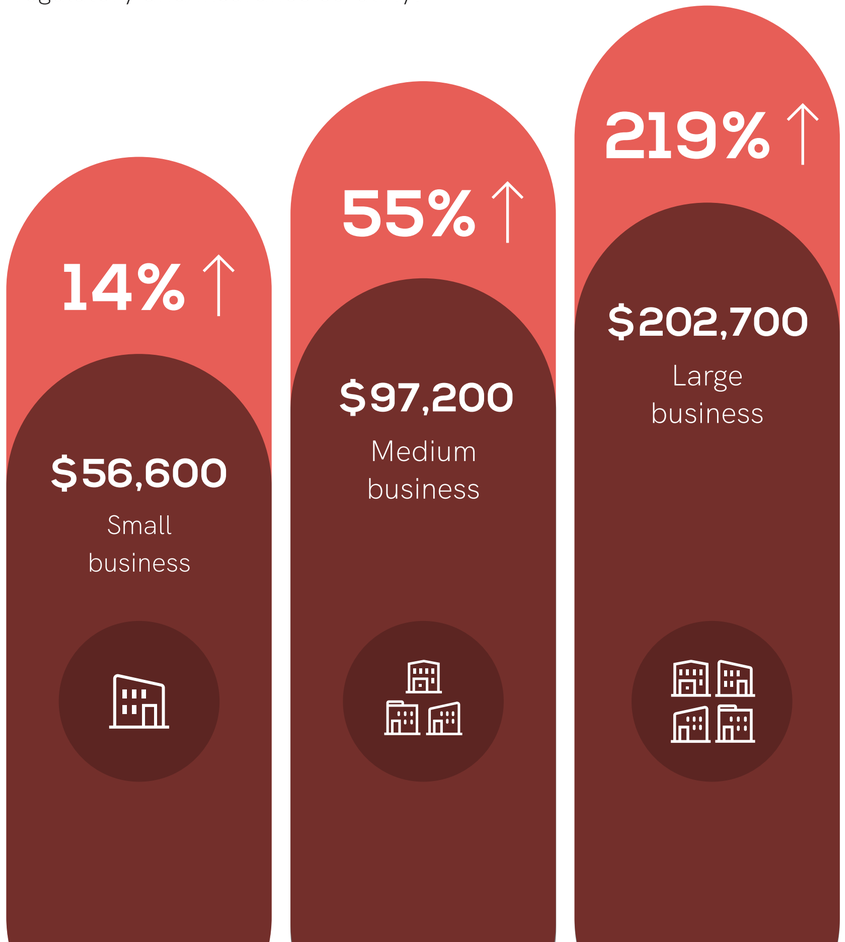
ASD reports significant increase in threat volume

During FY2024-25, the Australian Cyber Security Centre (ACSC) responded to more cyber security incidents, handled more calls from affected organisations, and issued significantly more proactive warnings about malicious activity than in the previous year.



Cost of cyber incidents up 55% for mid-market organisations

Medium and large organisations experienced the steepest growth in average financial impact per cyber incident, reflecting longer recovery times, greater business disruption, and increased regulatory and insurance scrutiny.



The problem isn't sophistication. It's execution

The Annual Cyber Threat Report shows that most cyber incidents in Australia exploit basic, preventable weaknesses rather than advanced techniques. Identity failures, poor patching, misconfiguration, phishing, and inadequate backups remain the most common attack paths.

In response, the ACSC continues to prioritise the Essential Eight as Australia's most effective baseline for reducing cyber risk, stating that proper implementation can prevent the majority of incidents it responds to.

However, as attackers increasingly blend in using legitimate credentials and built-in system tools, the challenge for many mid-market IT leaders is not a lack of security tooling, but having the people, processes, and expertise required to consistently operate, monitor, and prove Essential Eight uplift in day-to-day operations.

Cyber resilience in Australia: Reactive response vs operational consistency

In practice, the problem is rarely awareness or intent. Many organisations already have security tools and policies in place. Yet phishing simulations continue to show high credential capture rates, with exercises often escalating into administrative compromise.

This points to a recurring pattern: controls exist, but they are not applied or maintained consistently across users, endpoints, applications, and cloud environments.

Foundational controls degrade over time

Foundational security controls are not static. In corporate environments, as business requirements expand and the security threat landscape changes, maintaining least-privilege access within defined roles becomes increasingly challenging, patching schedules slip under operational pressure, and logging coverage becomes fragmented across platforms. Backup and recovery processes exist on paper but are rarely tested under real conditions.

As threat actors increasingly rely on legitimate credentials and built-in system tools, these gaps allow malicious activity to blend into normal operations and persist longer before detection.

> We see organisations with good tools in place, but without the operational consistency to keep controls effective over time. Cyber resilience is built in day-to-day execution, not one-off projects.
>
> **Garth Sperring, GM Network & Security, Nexon**

From tools to operational resilience

This changes the resilience equation. Effective cyber defence now depends less on reactive response and more on operational consistency. That is, the ability to run, monitor, and validate controls continuously, not episodically.

Regulators, boards, and insurers are reinforcing this shift. The question is no longer whether controls exist, but whether they are working, how failures are identified, and what evidence exists to demonstrate effectiveness over time.

For mid-market IT leaders without a dedicated CISO or large cyber team, the challenge is practical: how to structure cyber services so foundational controls remain sustainable, measurable, and defensible in day-to-day operations.

The execution gap in numbers

With more than 94,000 cyber-crime reports recorded by the ASD in FY2024-25, cyber risk in Australia is no longer episodic but a constant operational reality. While this figure spans organisations of all sizes, the ASD notes that medium and large organisations experience the greatest operational and financial impact when incidents occur.

Phishing simulations

credential capture

domain admin compromise

undetected until reported

Web app risk

misconfiguration

patchable vulnerabilities

Threat scale

YoY increase in DDoS incidents

malicious domain queries blocked upstream

Use case: From reactive alerts to operational control

A mid-sized Australian financial services organisation had invested in modern security tools but remained overwhelmed by alerts, slow investigations, and unclear response ownership, especially after hours.

The gap was execution. Controls existed, but detections were noisy, response paths fragmented, and incidents dragged on. By consolidating controls, tuning detections, and assigning clear ownership from triage through containment, security shifted from constant firefighting to repeatable operations.

With stable baselines in place, abnormal activity stood out faster, dwell time reduced, and control effectiveness became predictable rather than reactive.

Reactive response vs operational consistency: Two common security models

As Australian organisations mature their security posture, they typically operate in one of two broad models – point security solutions with reactive response or simplified security architecture with operational consistency and a trusted MSP.

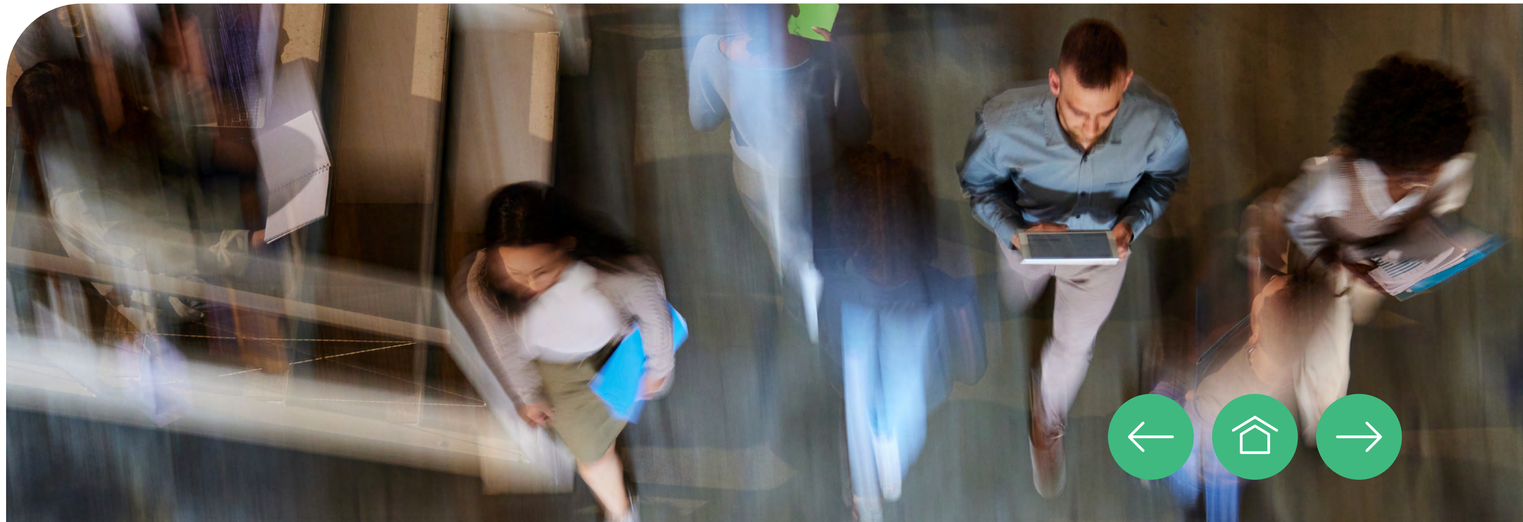
As threat actors increasingly rely on legitimate credentials and built-in system tools, resilience is determined less by what is deployed and more by how effectively it is run. For lean IT teams, simplifying architecture and shifting from reactive response to operational consistency is often the point where security outcomes begin to stabilise.

Point security solutions with reactive response

- Multiple standalone tools across identity, endpoint, email and cloud
- Alerts generated in volume, often without clear prioritisation
- Response ownership split across teams or escalated ad hoc
- After-hours coverage limited or best-effort
- Controls assessed periodically, not continuously
- Evidence assembled at audit or renewal time
- High operational load on internal IT teams

Simplified security architecture with operational consistency and a trusted MSP

- Core controls integrated across identity, endpoint and cloud
- Detections tuned to reduce noise and highlight material risk
- Clear ownership from triage through containment
- Defined response processes, including after-hours coverage
- Controls monitored continuously for drift and failure
- Evidence produced as part of normal operations
- Internal teams focused on improvement, not firefighting



What we're seeing: Early indicators from a GRC perspective

From a governance, risk and compliance (GRC) perspective, cyber resilience shows up first in day-to-day operations. In the above use case, the execution gaps that created alert fatigue and unclear response ownership also surfaced as assurance friction, fragmented evidence, and prolonged audit cycles. This illustrates a broader pattern we consistently see.

That is, when foundational controls are operated consistently and ownership is clear, GRC outcomes improve naturally. When they are not, compliance becomes reactive, evidence becomes difficult to assemble, and assurance effort increases.

Across Australian organisations, the most reliable early indicators are not about deploying more tools. They are about reviewing existing security, and how it can be measured and sustained across identity, endpoints, cloud platforms, and applications.

Grounded in recognised frameworks and obligations

Effective cyber governance does not exist in isolation. For Australian organisations, it is shaped by a growing set of regulatory, industry, and assurance requirements that demand both technical controls and defensible evidence.

Rather than treating these as separate compliance exercises, high-performing organisations use them as reference points to define risk tolerance, prioritise controls, and validate operating effectiveness over time.

From obligations to operational risk clarity

A recurring challenge for leaders is translating individual requirements into a coherent, operational risk posture.

From a GRC perspective, this starts with clearly articulating:

- The organisation's regulatory and contractual obligations
- The systems, identities, and data that materially support operations
- The level of risk the organisation is prepared to accept in each area

Once this risk profile is defined, control decisions become more consistent. Uplift efforts focus on the controls that matter most, evidence collection becomes simpler, and assurance discussions shift from justification to validation.

GRC signals we consistently see

From a GRC perspective, effective cyber resilience is revealed through a small number of operational signals. These signals show whether foundational controls are not only designed correctly, but are being run consistently, monitored continuously, and supported by evidence that stands up to scrutiny.

In practice, we see the strongest GRC outcomes when cyber programs are aligned to recognised frameworks such as ISO/IEC 27001, Essential Eight maturity expectations, and sector-specific obligations under the Security of Critical Infrastructure Act (SOCI) and CIRMP requirements, where applicable.

The GRC indicators below are the most reliable early signals we see when organisations move beyond point-in-time compliance toward sustained control effectiveness.

However, before these indicators can be interpreted meaningfully, organisations need a structured methodology to understand and articulate their risk profile. This typically involves four steps:

1 Identify

What it means

Map critical assets, systems, data, and business processes.

What to look for

Visibility of identities, endpoints, cloud, suppliers, and business-critical workflows.

2 Assess

What it means

Evaluate likelihood and impact of risks across these assets.

What to look for

Exposure from misconfigurations, access drift, unpatched systems, and staff behaviour.

3 Prioritise

What it means

Rank gaps based on real operational risk.

What to look for

High-impact gaps like weak identity controls, missing MFA, and inconsistent baselines.

4 Treat/validate

What it means

Implement and continuously test controls.

What to look for

Evidence that controls operate day-to-day, not just at audit time.

Once this baseline is established, the focus shifts to whether those controls can be operated consistently, monitored continuously, and demonstrated with evidence.

GRC indicators

These GRC indicators below reflect the shift from point-in-time compliance to defensible, operational resilience.

1

Essential Eight uplift becomes measurable and repeatable

Essential Eight uplift shifts from a static maturity goal to an operational process. Control baselines are defined, gaps are prioritised, and uplift is tracked continuously rather than assessed once.

- → Essential Eight uplift tracked through configuration, policy enforcement, and control evidence.
- → Progress measured over time rather than at audit checkpoints.
- → Uplift sustained through ongoing monitoring, not point-in-time remediation.

2

Assurance maturity

As assurance processes become more efficient and credible, audit and insurer engagements evolve from clarification-heavy reviews to evidence-driven validation.

- → Fewer audit exceptions and faster resolution cycles.
- → Insurer questionnaires supported by current, operational evidence.
- → Executive and board reporting aligned to live control health.

3

Control baselines are sustained, not just implemented

The strongest signal is sustainability. Identity, configuration, and logging baselines are monitored continuously, with drift identified early before it becomes an incident or audit issue.

- → Identity and configuration baselines defined and monitored.
- → Logging coverage and telemetry consistency maintained across platforms.
- → Control drift detected and corrected as part of normal operations.

Why these signals matter

From a GRC perspective, these signals determine whether cyber risk is governable, explainable, and defensible, not just technically managed.

When foundational controls are unstable, organisations experience alert overload and incident fatigue. Security teams are forced to triage high volumes of low-value alerts, slowing response times and increasing the likelihood that material risks are missed or detected late. This creates governance risk, not just operational inefficiency.

Where controls are consistently operated and measured, the signal-to-noise ratio improves. Automation and threat intelligence reduce manual triage, enabling faster investigation and response, which often compresses response timelines from minutes to seconds. This allows organisations to demonstrate not only that controls exist, but that incidents can be identified, prioritised, and acted on predictably.

The result is stronger assurance. Boards, regulators, and insurers gain confidence because risk is visible, response is repeatable, and evidence reflects real operating conditions rather than retrospective explanations.

> It’s no longer enough to surface alerts or tick compliance boxes. What matters is whether controls can actually be acted on, sustained, and proven to be working in day-to-day operations.
>
> **Mathew Boulenaz, Security Pre-Sales Lead, Nexon Asia Pacific**

Use case: From compliance to continuous assurance

In a large Australian not-for-profit organisation delivering essential disability and community services, cyber uplift focused on moving beyond static compliance toward continuous operational assurance.

Rather than relying on periodic assessments, the organisation established clear identity, endpoint and cloud baselines supported by centralised monitoring and detection. Regular system health checks, structured log retention and risk dashboards provided leadership with visibility into control performance and emerging trends.

This shift reduced assurance friction and strengthened confidence internally and externally by demonstrating that controls were not just present, but operating as intended.

Assessing growth risk in the volatile digital landscape

Across sectors, we are seeing the same concern surface in vCISO workshops, board briefings, and strategic planning sessions: How do we stay ambitious when AI-driven threats are evolving faster than our ability to predict them?

This is where the Corporate Resiliency Flexibility Ratio (CRFR) really changes the conversation. CRFR is a simple but powerful tool used to capture how much adaptive capacity an organisation truly has compared to the level of risk it's willing to take on in pursuit of its strategic goals.

In practice, it becomes a single, intuitive measure of three things leaders care about more than ever:

1. How much shock the business can absorb
2. How quickly it can adapt or recover
3. How much risk it can safely take on while still pushing for growth, innovation, and digital transformation

Boards increasingly want to know:

- Can we pursue aggressive digital growth without exposing ourselves to catastrophic cyber events?
- Are we over-investing in controls that slow innovation?
- Or underinvesting in resilience that protects revenue?

The CRFR gives them a single, interpretable signal that ties cyber governance to business value.

It helps justify decisions like expanding into new digital markets, accelerating AI adoption, increasing automation, and launching new customer-facing platforms.

In this age of AI-led threat risks, that clarity is invaluable. The CRFR becomes a bridge connecting business ambition with cyber risk exposure in a way that's practical, measurable, and aligned with how executives actually make decisions.

And as we keep applying it with clients, we're seeing its real value emerge. It doesn't just help organisations protect themselves. It gives them the confidence to move forward boldly, knowing their resilience is keeping pace with their ambition.

> The Corporate Resiliency Flexibility Ratio is the new litmus test for whether a business can grow confidently in a volatile digital landscape.
>
> **Mo Chowdhury, Principal Consultant Cyber Security, Nexon**

Evaluating your cybersecurity strategy: A 10-point self-diagnostic checklist

Boards, insurers, and regulators are no longer satisfied with point-in-time attestations. They expect ongoing evidence that security controls are operating effectively. At the same time, automation and low-cost hosting have amplified the scale and speed of threats, enabling attackers to operate at unprecedented volume. Predictably though, a majority of incidents still trace back to basic control failures rather than advanced techniques.

For emerging enterprise IT leaders, the question is not whether the right tools exist. It is whether there are enough people, repeatable processes, and defensible evidence to run those controls well, day in and day out.

Use this checklist to help identify where controls are strong, where they are fragile, and where external support can deliver the greatest uplift.

10-point self-diagnostic checklist

- ❶ **Identity hygiene**
  Are user and privileged accounts protected with strong MFA, least-privilege access, and regular role-based control reviews to assess if access has accumulated over time?
- ❷ **Patch cadence**
  Are critical vulnerabilities consistently remediated to ensure exploits are actively being targeted today and are being patched with a priority across endpoints, servers and cloud services, even during busy operational periods?
- ❸ **Email and domain security**
  Are phishing protections, domain controls, and authentication standards actively monitored and adjusted as attack techniques evolve?
- ❹ **EDR and telemetry**
  Do endpoints, identities, and cloud platforms generate reliable telemetry (enables detection, investigation, and response, not just alerting) that is correlated centrally and enriched with Threat Intelligence data?
- ❺ **24×7 detection and response**
  Is there named on-call coverage with clear escalation paths, measured detection, and containment times, and after-hours response capability?
- ❻ **Exposure management**
  Are misconfigurations, external exposures, and risky services identified continuously, prioritised by impact, and reduced systematically?
- ❼ **Continuity readiness**
  Have incident runbooks, crisis communications, and tabletop exercises been tested in the last 12 months, not just documented?
- ❽ **Compliance reporting**
  Is control evidence produced regularly in a format boards, regulators, and insurers accept, rather than assembled only at renewal or audit time?
- ❾ **User resilience**
  Do phishing simulations and training show improving outcomes over time, with corrective action taken when risk indicators rise?
- ❿ **Change control**
  Are joiner-mover-leaver processes enforced within SLAs, with administrative access time-bound, approved and logged?

Balancing cyber risk with commercial reality

For IT leaders, every security decision sits at the intersection of risk, cost, and operational impact. The real cost of a cyber incident is not measured solely in remediation effort. It includes operational downtime, lost productivity, regulatory scrutiny, insurance consequences, and erosion of stakeholder and, for some organisations, customer trust.

In many cases, these impacts far outweigh the perceived savings of deferring or underinvesting in foundational controls.

Forward-thinking leaders approach cyber resilience as an optimisation exercise. They prioritise controls that materially reduce risk, align investment to likely attack paths, and focus spend where failure would have the greatest business impact. Clear risk articulation, supported by ROI analysis and defensible business cases, enables security investment to be positioned as a business enabler rather than a discretionary cost.

Where external support adds the most value

For many organisations, the biggest lift comes from augmenting internal teams rather than replacing them. External support is typically most effective where scale, specialisation, or 24×7 coverage is required.

- **24×7 security operations with ownership of outcomes:** Alerts are triaged, investigated, and acted on by named analysts who own incidents through containment and recovery, not simply escalated as tickets.
- **Threat hunting and detection tuning:** Continuous improvement to reduce alert fatigue and missed incidents.
- **Incident response readiness:** Rapid mobilisation, forensic support, and insurer-aligned response coordination.
- **Identity and cloud posture uplift:** Hardening of identity platforms, least-privilege enforcement and configuration baselines.
- **Surge capacity:** Prioritising what controls to configure or patch first to reduce exposure without increasing headcount.

Assessing when external cyber support adds value

To help assess whether external cyber support is appropriate, IT leaders can evaluate their current operating model against the criteria below.

Assessment criteria	Internal-only model	Externally-supported model
Scale	Limited by team size and competing priorities. Coverage often degrades during leave or major projects.	Scales on demand. Peak incidents, uplift programs, and after-hours response are absorbed without increasing headcount.
Specialisation	Generalist skills dominate. Deep expertise in identity, IR, threat hunting, or compliance is often ad hoc or outsourced reactively.	Access to specialised skills across detection, incident response, compliance, and risk without permanent hires.
Coverage	Business-hours focused. After-hours response depends on on-call staff or best-effort escalation.	Continuous 24×7 monitoring and response with defined ownership and escalation paths.
Integration	Tools and processes evolve independently. Visibility and telemetry can be fragmented across platforms.	Integrated detection, response, and reporting across identity, endpoint, cloud, and SaaS environments.
Operational consistency	Controls depend heavily on individual effort and institutional knowledge. Drift accumulates over time.	Controls are run, monitored, and validated as repeatable operational processes.
Evidence and assurance	Evidence assembled periodically for audits, renewals, or incidents.	Evidence produced continuously as part of normal operations.

> Everything starts with understanding the mandate – what obligations apply to your organisation, and what level of risk and control those requirements actually demand.
>
> **Mo Chowdhury, Principal Consultant Cyber Security, Nexon**

Turning cyber exposure into foundational maturity: Get protected and stay protected

For many Australian organisations, cyber risk is already well understood. What's harder is converting that awareness into controls that actually hold up in day-to-day operations.

Nexon approaches this challenge through a structured, subscription-based cyber security framework designed to simplify protection, strengthen defences, and support ongoing compliance.

Rather than adding more tools, the focus is on establishing strong foundations, sustaining them operationally, and strengthening resilience over time through clear service plans with defined outcomes.

This creates a practical pathway from exposure to maturity, aligned to how organisations actually operate.

Clear subscription-based service plans

Nexon Cyber is delivered through clear, subscription-based service plans that define service delivery, SLAs, and outcomes across the full cyber lifecycle. These plans remove the guesswork common in traditional cyber security investment and allow organisations to select the level of protection and operational support that fits their risk profile and regulatory obligations.

The service plans apply across all stages of protection.

Essentials	Core protection for organisations requiring baseline visibility with defined SLAs of cyber posture and incident response.
Advanced	SOC-supported monitoring with SLA-backed response and remediation, suited to organisations with stronger compliance and governance requirements.
Premium	SOC-supported monitoring, SLA-backed response and remediation including vulnerability management for highly regulated organisations and government agencies requiring higher levels of security maturity.
À la carte	Tailored services for complex environments or specific operational needs.

Service plans can be augmented with additional capabilities, including vCISO support, incident response, penetration testing, and compliance services, as organisational needs evolve.

A three-stage operating model for cyber resilience

Cyber resilience is not delivered through a single project or control uplift. It is built by establishing strong foundations, operating them consistently, and validating their effectiveness under real-world conditions.

Nexon structures cyber services around three operational stages that reflect how risk actually emerges and is managed over time.

Get protected:

Rapidly harden identity and access

Stay protected:

Sustain protection through additional detection and response services

Don't get caught out:

Test, validate, and prepare for real-world incidents

The first step is reducing the most common attack paths observed in real incidents.

Identity hardening:
Enforce multi-factor authentication for all users and privileged roles, apply conditional access, and remove standing admin access through least-privilege and PAM workflows.

Platform hardening:
Apply secure baselines across endpoints, email, and DNS, and prioritise remediation of high-severity exposures.

Outcome:
Fewer successful phishing attacks, credential replay, and commodity malware. Immediate uplift in control maturity against Essential Eight fundamentals.

A three-stage operating model for cyber resilience

Cyber resilience is not delivered through a single project or control uplift. It is built by establishing strong foundations, operating them consistently, and validating their effectiveness under real-world conditions.

Nexon structures cyber services around three operational stages that reflect how risk actually emerges and is managed over time.

Get protected:

Rapidly harden identity and access

Stay protected:

Sustain protection through additional detection and response services

Don't get caught out:

Test, validate, and prepare for real-world incidents

Once foundations are in place, the focus shifts to operating them consistently. These capabilities are available as optional, pick-and-choose add-ons that allow organisations to extend protection where risk and internal capacity require it, rather than adopting a one-size-fits-all model.

MSP Owned response:
24×7 detection and response with Australia-based analysts who take ownership from triage through containment, supported by use-case-driven detections, noise suppression, and proactive threat hunting across identity, endpoint, SaaS, and cloud environments.

Continuous assurance:
Ongoing vulnerability and configuration management, with continuous control monitoring and operational evidence such as detection and containment performance.

Outcome:
Reduced dwell time and blast radius, with evidence that controls are operating as intended and the incident has been resolved.

A three-stage operating model for cyber resilience

Cyber resilience is not delivered through a single project or control uplift. It is built by establishing strong foundations, operating them consistently, and validating their effectiveness under real-world conditions.

Nexon structures cyber services around three operational stages that reflect how risk actually emerges and is managed over time.

Get protected:
Rapidly harden identity and access

Stay protected:
Sustain protection through additional detection and response services

Don't get caught out:
Test, validate, and prepare for real-world incidents

Resilience depends on how controls perform under pressure, and whether organisations have access to senior security leadership, such as a vCISO, to guide decision-making, escalation, and risk prioritisation when it matters most.

Control validation:
Regular breach-and-attack simulation, purple-team exercises, and targeted penetration testing focused on preventable weaknesses such as identity hygiene, misconfiguration, and exposed services.

Incident readiness:
Practised incident runbooks, tabletop exercises, supplier and OT visibility, and vCISO guidance aligned to board and insurer expectations.

User resilience and cultural awareness:
Ongoing security awareness training and phishing simulations that reinforce expected behaviours, measure real-world risk, and trigger corrective action when user-driven exposure increases.

Outcome:
Stronger response readiness, increased confidence from boards and insurers, and smoother renewals supported by defensible evidence.

Why a managed SOC changes the resilience equation

For lean IT teams, the gap is typically coverage, specialist depth, and the ability to respond decisively when something goes wrong. A managed Security Operations Centre (SOC) addresses this gap by providing continuous monitoring, investigation, and response ownership that most emerging enterprises cannot sustain internally.

A mature managed SOC operates as an extension of the organisation, with Australia-based analysts who understand the environment, tune detections over time, and take responsibility from triage through containment. This reduces alert fatigue, shortens dwell time, and ensures incidents are actively managed rather than escalated and abandoned.

Critically, a managed SOC also underpins governance and assurance. Operational evidence, response metrics, and control health reporting are produced as part of normal operations, supporting board visibility, insurer confidence, and regulatory expectations without adding reporting overhead to without adding reporting overhead to internal teams.

Use case: From exposed foundations to proactive risk reduction

A large Australian not-for-profit organisation delivering essential disability and community services identified growing risk across identity, endpoints, and cloud platforms, but lacked the internal capacity to monitor and respond to threats around the clock.

Initial focus was placed on strengthening foundations. Identity protections were standardised, multi-factor authentication was enforced across staff and privileged roles, and endpoint hygiene was improved through consistent policy baselining and remediation.

With baseline controls stabilised, the organisation moved to sustained protection. Centralised detection and response enabled continuous monitoring across identity, endpoint, and cloud activity, supported by clear ownership from triage through containment. Over time, this shifted security from reactive clean-up to proactive risk reduction.

Achieving sustainable protection in 2026: From preventable to predictable

Australia's cyber threat landscape is no longer defined by unknowns. The evidence from national reporting and real-world operations shows that most incidents continue to stem from familiar, preventable weaknesses. The differentiator is no longer awareness. It is whether organisations can keep foundational controls operating consistently over time.

For emerging organisations, this is a practical challenge. Limited headcount, fragmented tooling, and growing regulatory pressure make it difficult to sustain Essential Eight uplift, detect failure early, and demonstrate control effectiveness when it matters most.

Your provider must do more than raise an alert and walk away. What matters is whether you can act on it quickly, own the outcome, and reduce the risk before it turns into real damage.

Mathew Boulenaz, Security Pre-Sales Lead, Nexon Asia Pacific

As organisations increasingly explore AI-enabled systems and automation in 2026 and beyond, the importance of strong cyber foundations becomes even more pronounced. AI amplifies both opportunity and risk, accelerating productivity while increasing the potential impact of identity compromise, data leakage, and misconfiguration.

Secure AI adoption depends on the same fundamentals outlined throughout this guide: strong identity controls, clear data governance, reliable logging, and continuous assurance. Without these guardrails in place, AI systems can inherit and magnify existing weaknesses.

For this reason, security posture assessments and control validation are becoming a critical precursor to AI integration. Organisations that establish clear security baselines before deploying AI are better positioned to innovate safely, meet regulatory expectations, and protect sensitive data as adoption accelerates.

Nexon helps Australian organisations bridge that gap. Through structured service plans, operational visibility, and local expertise, organisations can move from reactive defence to predictable, measurable cyber resilience.

Assess your exposure – Request a Nexon Cyber Risk Assessment

1300 800 000

nexon.com.au/cyber

Follow **nexonap**