Tautsec Pty Ltd
[redacted]
27 August 2025

SUBMISSION TO HORIZON 2 – CYBER SECURITY STRATEGY 2023-2030

Dear Minister,

Tautsec Pty Ltd welcomes the opportunity to contribute to the development of Horizon 2 of the 2023–2030 Australian Cyber Security Strategy.

We are a proudly Australian cyber security company dedicated to protecting the engine room of our nation's economy: small and medium-sized enterprises (SMEs). Our platform helps SMEs access appropriate cyber insurance and provides free access to an integrated compliance tool, available either alongside insurance or as a standalone service, designed to quantify risk, educate business owners, and automate workflows against the Essential 8 and international standards such as the NIST CSF.

We commend the Australian Government on the comprehensive 2023-2030 Australian Cyber Security Strategy, particularly the ambition to provide SMEs and not-for-profits (NFPs) with accessible, cost-effective pathways to uplift their cyber resilience and welcome the chance to support the Horizon 2 Action Plan.

This submission focuses on Shield 1 of the Strategy, "Strong businesses and citizens," with a particular emphasis on practical and effective measures to uplift the cyber resilience of Australian SMEs. We believe that with the right policy settings, Australia can create a step-change in the security posture of our small business community, fostering innovation, trust, and broad economic growth.

SMEs need a simple pathway to compliance and assurance that builds supply-chain confidence. Enabling step-by-step progress to recognised certification strengthens the economy, while tailored cyber insurance provides the safety net to recover from incidents.

The SME Cyber Security Challenge

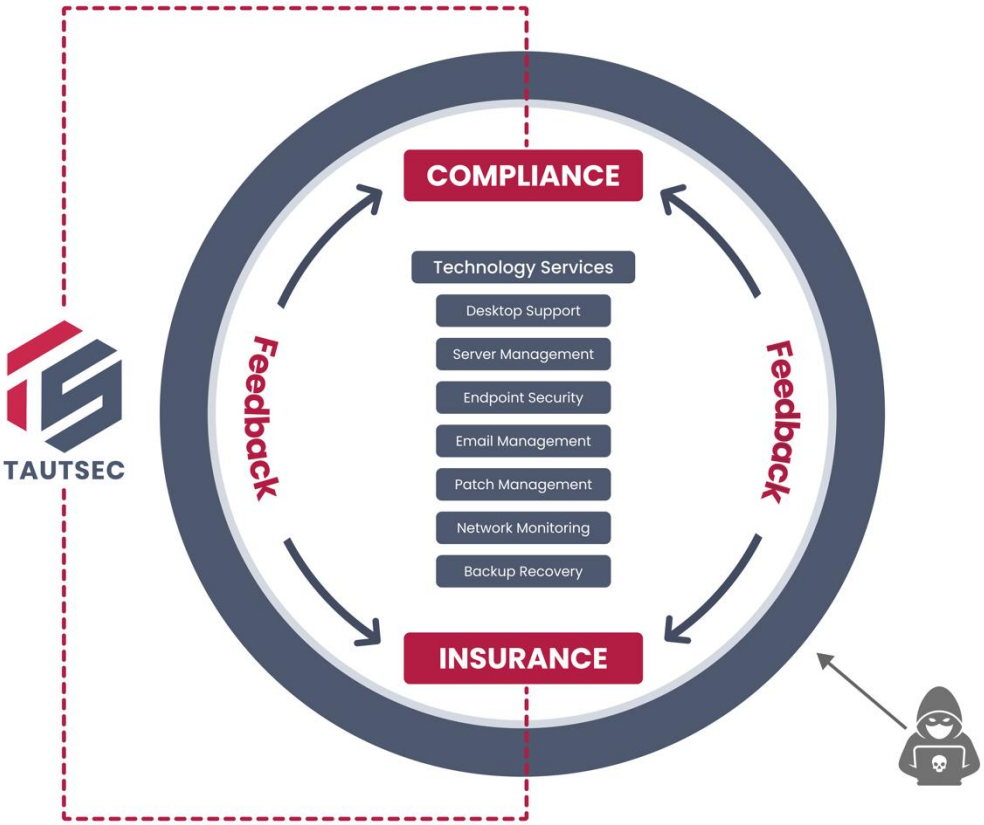
The Horizon 2 Policy Discussion Paper correctly identifies the unique vulnerabilities of SMEs. These businesses are attractive targets for malicious actors and often provide the gateway for larger enterprises through their supply chain yet are often the least equipped to defend themselves. As the Discussion Paper highlights, existing standards and frameworks are often too complex or resource-intensive for smaller entities to apply. From our frontline experience, the primary barriers for SMEs are not a lack of will, but a lack of:

- **Resources:** Limited budgets preclude the hiring of dedicated IT security staff or the procurement of expensive enterprise-grade security solutions.
- **Time:** SME owners are time-poor, juggling multiple roles. They cannot afford to become cyber security experts overnight.
- **Expertise:** The cyber security landscape is complex and constantly evolving. Navigating the jargon, understanding the threats, and implementing the correct controls is a significant challenge.

This has created a market where Commonwealth government intervention could reap immediate benefits. Most available cyber security solutions are designed for large enterprises with dedicated security teams and substantial budgets. While now 2 years old, the ACSC's Small Business Survey found 63% of Australian SMEs spent less than $1,000 annually on cyber security. This leaves a gap in the market for solutions that are accessible, affordable, and effective for the SME sector. The result is a large and vulnerable attack surface that puts the Australian economy at risk and reduces confidence in Government's penetration in cyber security awareness.

Proposed Policy Approach for Horizon 2

To address this challenge, we propose a policy framework for Horizon 2, Shield 1, that moves beyond awareness campaigns and encourages the widespread adoption of a new class of automated, "actively managed" cyber security solutions tailored for SMEs. We feel an approach which provides the "top layer" of protection through educated governance, combined with a "bottom layer" protection of cyber insurance, with a closed feedback loop, would provide invaluable data to help shape the future direction of the strategy.



Response to Para 2.3 – Outlook for Horizon 2

Question: "Conceptual framework for evaluating outcomes…"

Response: Our platform provides "Top-level - **Governance**" based on global best practice standards, combined with "Last line of defence - **Insurance**", with a **feedback loop** driving user behaviour, rewarding pro-active participation in elevating cyber posture across the community.

1. Encourage Adoption of "SME-Ready" Cyber Security Solutions

The Government has an opportunity in Horizon 2 to stimulate adoption of baseline cyber security capabilities through regulation, endorsement or policy guidance that:

- **Endorses a national 'baseline' SME cyber security standard** – a simplified framework that allows businesses to meet their obligations under privacy, critical infrastructure, and corporate governance laws without excessive compliance cost. This baseline should support a national assurance pathway, giving SMEs a roadmap from basic hygiene to certification with measurable milestones. While the Essential 8 is far more accessible than international standards, it is still too complex for SME adoption without digital tools that generate recommendations for cyber security improvements.
- **Encourages adoption through procurement and certification incentives** – e.g., recognising certified SME solutions within government tenders, insurance pricing, and supply-chain risk management.
- **Integrates technical solutions with awareness programs** – ensuring government campaigns such as *Act Now. Stay Secure* are paired with easy-to-deploy, practical tools that operationalise secure behaviours.
- **Supports innovation and local capability** – promoting homegrown solutions that can scale nationally and be exported internationally, thereby strengthening Australia's sovereign cyber industry base.

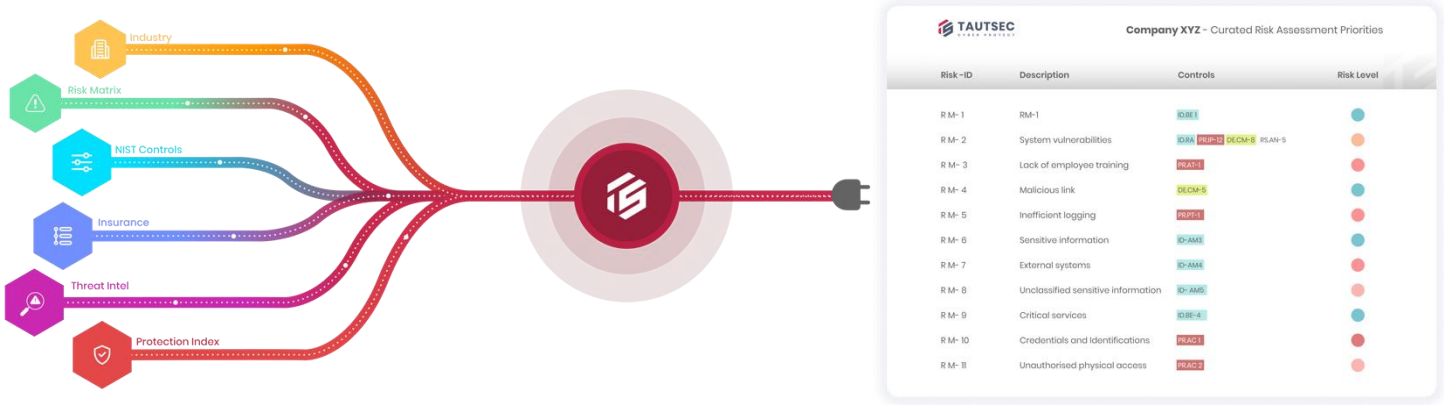
2. Incentivise Adoption through a Government Co-investment Model

To drive the uptake of "SME-Ready" solutions, we propose a government co-investment model, such as an SME grant program or tax incentive. This would help to de-risk the initial investment for SMEs and accelerate the adoption of best-practice cyber security. Encouraging and educating small business on the benefits of Cyber Insurance, not only to recover from an incident, but to inform the future direction of risk mitigation strategies, when combined with an effective risk mitigation tool, could significantly "move the needle" as the policy roadmap develops. A co-investment model lowers entry barriers and encourages SMEs to advance along a certification pathway, with compliance maturity unlocking insurance benefits and reducing risk.

This approach has several advantages:

- It is market-based, fostering innovation and competition among Australian cyber security providers to develop qualifying solutions.
- It empowers SMEs with the tools they need to protect themselves, rather than imposing a complex regulatory burden.
- It has a low upfront cost and provides a clear return on investment for the government, by reducing the incidence and cost of cybercrime affecting SMEs.
- It benefits Small Business through providing tools to recover and respond from an incident.

Cyber security is a complex and complicated field. The response to-date has been a complex and complicated cyber security consultancy-focused landscape. Horizon 2 presents a timely and unique opportunity to create standardised metrics utilising cross-mapping of regulatory frameworks to build a simple solution to a complex and dynamic environment. Our proposed solution which ingests information from NIST, ACSC, ISO, NIST Informative References, NIST OSCAL, Insurance Claims, Real-Time Threat Intel, and an adaptive algorithm to create a simple to use, meaningful solution to baseline Cyber Risk.



Response to Para 2.1 – Outlook for Horizon 2

Question: "Strategic factors for cyber security under Horizon 2."

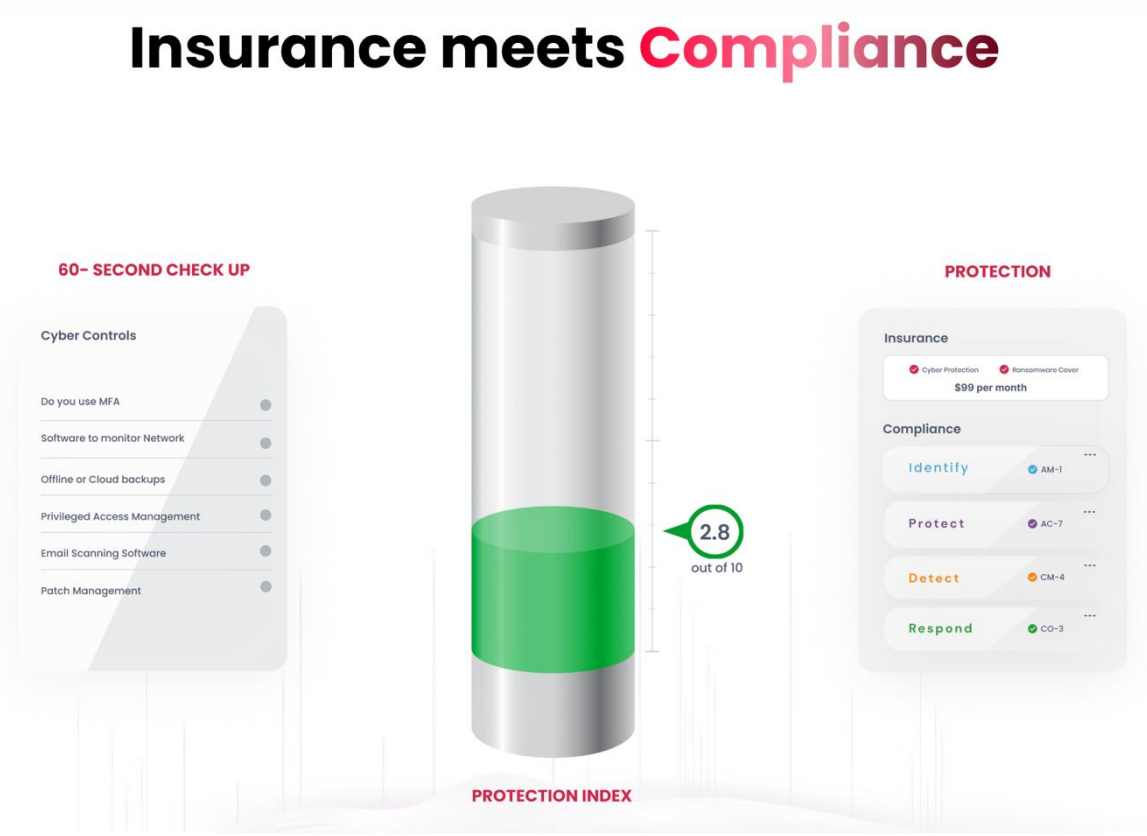
Response: Complex Input from multiple, complex and dynamic inputs translated into effective, easy-to-understand workflows.

3. Specific Recommendations for Government Action

To achieve this ambition, we recommend the Government:

1. **Develop and endorse an SME-tailored cyber certification scheme** – incorporating practical tools that meet baseline controls and outline a clear pathway to assurance. Approved platforms would let SMEs plug in resilience confidently and at low cost.
2. **Mandate minimum supply-chain cyber requirements** – requiring SME suppliers to larger firms and government agencies to hold a recognised SME certification. This drives uplift across the economy without imposing onerous regulation.
3. **Provide adoption incentives** – including grants, tax offsets, or insurance premium reductions for certified products and services that demonstrably uplift cyber maturity.

4. **Embed technology solutions in awareness campaigns** – linking public messaging with approved, easy-to-use tools so that individuals and small organisations can immediately act on guidance.
5. **Lowering the barrier to entry for cyber governance** – Encouraging adoption of cost-effective risk-mitigation platforms which "bracket" traditional cyber tools. This dual structure supports national resilience: governance provides a pathway to certification, while insurance mitigates financial impact. Together, they help SMEs prevent and withstand threats, protecting jobs and the economy.



Response to Para 3.1 – Strong businesses and citizens

Questions: "…Standards … Insurance … Best Practise…."

Response: Simple online Cyber Insurance (left side) **linked** to Cyber Controls (right side), with simple, yet comprehensive standardised **Risk Metric** (Protection Index).

Alignment with the Cyber Security Strategy

This proposed approach directly supports the objectives of Shield 1 of the 2023-2030 Australian Cyber Security Strategy. By fostering the development and adoption of SME-Ready solutions, the government can:

- **Empower businesses:** Provide SMEs with the practical tools they need to defend themselves in a complex threat environment. This includes a government-endorsed pathway to certification, ensuring SME investments deliver measurable improvements and signal resilience to supply-chain partners.
- **Reduce barriers:** Lower the cost and complexity barriers that currently prevent SMEs from adopting effective cyber security measures.
- **Educate business owners:** Distribute timely, targeted and concise messaging across the business community, elevating Australia's Cyber awareness.
- **Strengthen resilience:** Improve the ability of Australian businesses to prevent, and bounce back from, cyber-attacks, thereby strengthening the entire economy. Resilience must be both operational and financial. By combining certification-driven assurance with access to specialist cyber insurance, SMEs can both elevate their defences and mitigate the unavoidable costs of an incident. This dual approach provides confidence to business owners, investors, and the wider economy.

Conclusion

Tautsec is committed to working in partnership with the Australian Government to build a more cyber-resilient nation. Focusing on the unique needs of the SME sector and fostering a market for innovative, accessible, and automated security solutions, will see us achieve the ambitious goals set out in the 2023-2030 Cyber Security Strategy and keep Australians safe online.

We thank you for the opportunity to provide this submission and would be pleased to offer further information or participate in workshops to assist in the development of the Horizon 2 Action Plan.

Yours Sincerely,

[redacted]

[redacted]

TautSec Pty Ltd

Note on sourcing: *In preparing this submission, we have engaged with The Department of Home Affairs, Australian Signals Directorate's Australian Cyber Security Centre (ACSC), The Council of Small Business Organisations Australia (COSBOA), Australian Chamber of Commerce and Industry (ACCI) and the National Officer of Cyber Security (NOCS).*