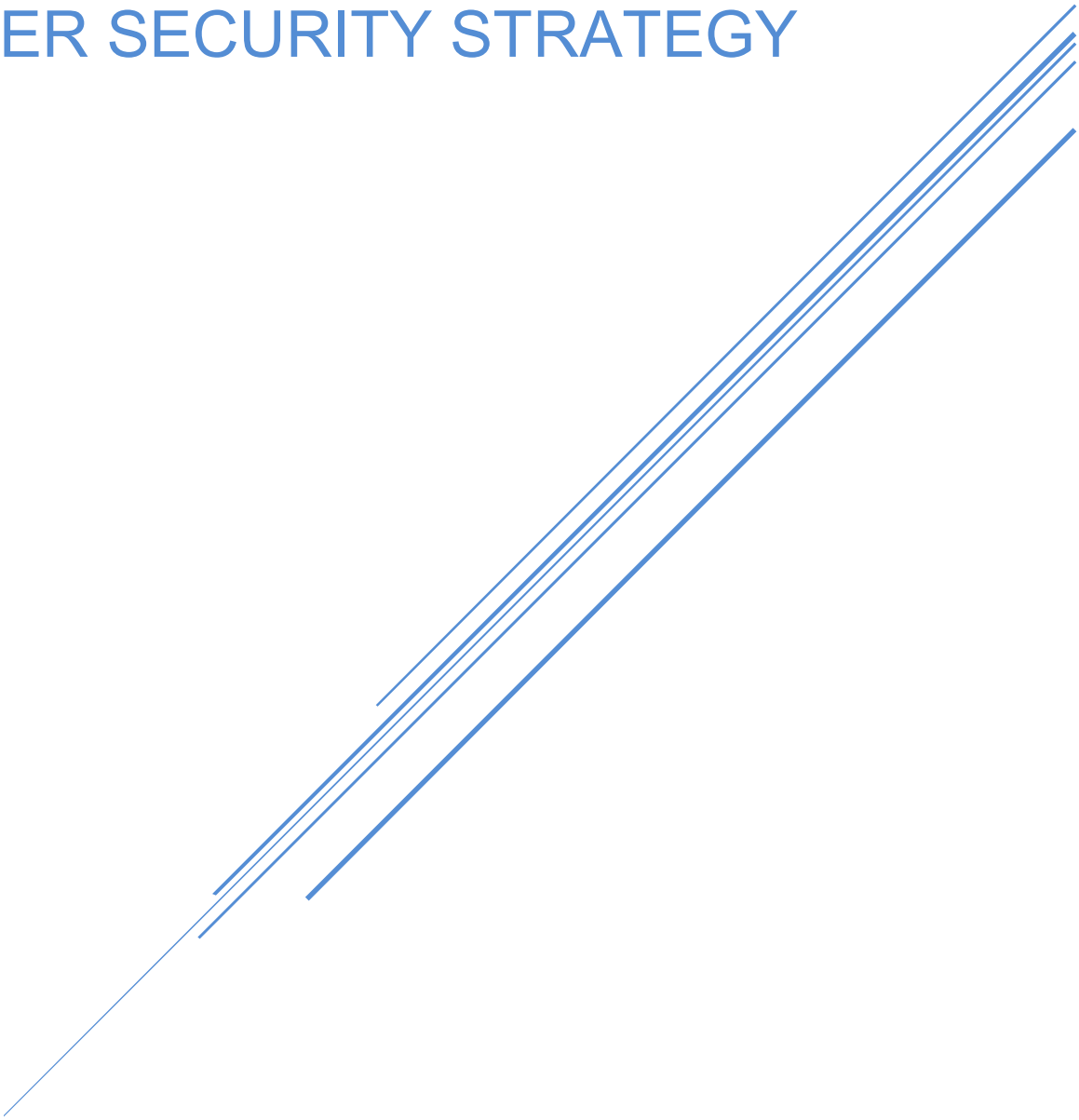
OPENXCHANGE

SUBMISSION TO HORIZON 2 OF THE 2023–2030 AUSTRALIAN CYBER SECURITY STRATEGY



Executive Summary

OpenExchange is a nationally distributed startup founded by professionals with extensive experience in cyber risk, financial services, technology compliance, and regulatory governance. We work closely with small to mid-sized enterprises (SMEs), regulated entities, and public sector partners to modernise risk operations and cyber capability across Australia.

We commend the Australian Government's consultative approach in the development of Horizon 2 and welcome the opportunity to contribute practical, industry-informed insights. This submission addresses the questions outlined in Appendix A of the Horizon 2 Discussion Paper and makes evidence-based recommendations across all six of the Strategy's core cyber security Shields.

As a startup embedded in the operational realities of risk and compliance across Australia, OpenExchange believes the success of Horizon 2 lies in practical delivery, regulatory coherence, and shared ownership of cyber resilience.

We recognise Horizon 2 as a pivotal opportunity to enhance national cyber resilience and digital trust. As a practitioner-led organisation deeply engaged with industry and community, OpenExchange is well placed to offer commentary on the challenges and implementation realities facing Australian businesses, particularly in regulated and risk-sensitive sectors.

We are supportive of the Government's intent and remain available to assist further in the implementation of initiatives arising from this consultation process.

Strategic Outlook for Horizon 2

Trends and Technology Disruptors
The pace of digital transformation—spanning generative AI, quantum computing, digital identity, and data brokerage ecosystems—will continue to alter Australia's cyber risk profile over the coming years. These shifts demand anticipatory regulation, modernised compliance infrastructure, and greater coordination between policy, risk operations, and business execution.

Recommendation:
Establish a national public–private foresight advisory council on emerging cyber risks, chaired by the National Cyber Security Coordinator, with representation from startups and SMEs alongside enterprise and government.

Public Sector Coordination

Scaling What Works
We encourage the replication of successful jurisdictional models across states and territories. Examples include NSW's shared services for cyber training and Victoria's cyber resilience benchmarking frameworks.

Recommendation:
Mandate harmonisation of regulatory reporting portals and thresholds across sectors and jurisdictions to reduce duplicative compliance burdens and encourage voluntary reporting.

Evaluation and Accountability

Cyber Security Policy Evaluation Model
The model appropriately reflects causal relationships between cyber posture and economic security. However, greater granularity is required for small business recovery metrics, victim remediation outcomes, and regulatory intervention effectiveness.

Recommendation:
Develop metrics to assess the maturity and success of cyber uplift efforts in SMEs, and incorporate these into national reporting dashboards to inform future investment.

Shield-Level Recommendations

Shield 1: Strong Businesses and Citizens

- **Cyber Awareness and Literacy**
  The proliferation of cyber awareness messaging across platforms risks fragmentation and fatigue. There is a clear need for consistent, tiered messaging aligned to digital literacy levels.

  Recommendations:

  - Fund co-branded awareness programs in partnership with fintech and regtech providers who already support SMEs and NFPs.
  - Expand Cyber Wardens and “Train-the-Trainer” programs through industry associations and local councils.

- **Uplifting SME and NFP Resilience**
  Cyber risk frameworks are often inaccessible to smaller organisations due to complexity and resourcing constraints.

  Recommendations:

  - Introduce a national "Cyber Ready for Business" accreditation scheme for SMEs, modelled on ASIC’s RG 271 and AS ISO/IEC 27001 Lite.
  - Provide direct micro-grants or tax offsets to cover vendor-certified basic cyber controls (e.g. MFA, backups, response planning).

- **Ransomware and Insurance**
  Most SMEs OpenExchange engages with lack viable insurance options due to price, exclusions, or claims complexity.

  Recommendations:

  - Co-invest in market-shaping pilots with insurers to offer bundled cyber insurance for accredited SMEs.
  - Release updated ransomware mitigation playbooks targeted at non-technical leaders in business.

Shield 2: Safe Technology

- **Minimum Standards and Consumer Protection**
  A consistent, trustworthy technology labelling scheme is essential to restore consumer trust and support

procurement decisions.

Recommendations:

- Introduce mandatory baseline standards for consumer IoT and connected devices by 2027.
- Co-design an “Australian Secure by Design” product label, aligned with international frameworks.

- **Managing Technology Vendor Risk**
  Small entities lack the tools and guidance to understand and manage foreign ownership or influence.

  Recommendation:
  Develop a vendor risk assessment toolkit specifically for SMEs and local councils, embedded in government procurement templates.

Shield 3: World-Class Threat Sharing and Blocking

- **Operationalising Threat Sharing**
  Many SMEs do not participate in existing threat sharing initiatives due to lack of awareness or perceived irrelevance.

  Recommendations:

  - Fund pilot Information Sharing and Analysis Centres (ISACs) in underrepresented sectors including professional services, regional healthcare, and education.
  - Develop template threat briefings in plain English tailored to smaller organisations and non-technical boards.

- **Blocking at Scale and Researcher Protections**
  Safe browsing warnings and automated blocking technologies can significantly reduce harm if deployed nationally.

  Recommendation:
  Mandate deceptive domain and phishing protection at the ISP level, with real-time support from the National Cyber Intel Partnership.

Shield 4: Protected Critical Infrastructure

- **Clarity and Proportionality under SOCI**
  OpenExchange clients in sectors adjacent to designated critical infrastructure often mirror those obligations without equivalent support or guidance.

Recommendations:

- Expand SOCI-style implementation toolkits for aligned industries, such as aged care, vocational training, and payroll providers.
- Increase capacity-building grants for small operators to meet regulatory expectations without undue cost or complexity.

Shield 5: Sovereign Capabilities

- **Workforce Development and Transition Pathways**
  Our work across industry confirms that risk professionals, auditors, and operations leads are well placed to transition into cyber roles.

  Recommendations:

  - Fund national “Cyber Career Conversions” that target mid-career professionals from banking, compliance, and risk.
  - Launch micro-credentialling platforms that allow on-the-job pathways aligned to ASD, ACS and ISO competency levels.

- **Research and Innovation Ecosystem**
  There is opportunity to further bridge applied research and commercial product development in security analytics, secure identity and automation tooling.

  Recommendation:
  Establish a Sovereign Cyber Innovation Stream under the Industry Growth Program focused on emerging regtech, AI assurance and data protection solutions.

Shield 6: Resilient Region and Global Leadership

- **Regional Cooperation and Standards Alignment**
  Cyber RAPID is a valuable foundation for strategic influence in the region.

  Recommendations:

  - Expand regional deployments through industry secondments and joint capability-building missions with ASEAN partners.
  - Support alignment on standards for cross-border identity, threat attribution and data transfer with Indo-Pacific allies.