KPMG

# Charting new horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

## KPMG submission

KPMG Australia, August 2025
**KPMG.com.au**

# Contents

# Executive summary

As a leading professional services firm, KPMG Australia (KPMG) is committed to meeting the requirements of all our stakeholders, not only the organisations we audit and advise, but also employees, governments, regulators, and the wider community. We strive to contribute in a positive way to the debate that is shaping the Australian economy and we welcome the opportunity to provide a submission to the Department of Home Affairs' consultation on *Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy*.

This submission builds on KPMG's previous work in this space, including our 2023 submission in response to the *2023-2030 Australian Cyber Security Strategy Discussion Paper*[1] and September 2021 submission in response to the *Strengthening Australia's cyber security regulations and incentives* discussion paper.

This submission outlines a number of recommendations aimed at addressing emerging threats, uplifting community awareness, and enhancing Australia's sovereign capabilities in order to uplift Australia's cyber maturity across Horizon 2.

KPMG emphasises the importance of inclusive cyber security awareness campaigns that resonate with diverse demographic groups. We also note the need for tailored support for small businesses and not-for-profit organisations, recognising their limited resources and unique threat environments. Additionally, as part of a successful cyber security strategy, Australia needs a modern, enforceable data protection framework aligned with global standards.

To strengthen Australia's cyber resilience, KPMG proposes enhanced cross-sector collaboration, a national framework for managing foreign ownership, control, or influence risks, and the development of a principle-based cyber security framework supported by a national information-sharing hub. The submission also calls for the implementation of a national cyber workforce strategy that promotes diversity and supports startups through inclusive procurement reform.

We stand ready to help our clients, governments and the community be prepared for the unique cyber security challenges identified in the discussion paper, ultimately working towards a strengthened cyber security capability for Australia.

Yours sincerely,

[redacted]
KPMG Australia

[1] KPMG Submission - 2023-2030 Australian Cyber Security Strategy Discussion paper

# Background

## About KPMG

KPMG is a global organisation of independent professional firms, providing a full range of services to organisations across a wide range of industries, governments and not-for-profit sectors. We operate in 143 countries and territories and have more than 265,000 partners and employees working in member firms around the world. In Australia, KPMG has a long tradition of professionalism and integrity combined with our dynamic approach to advising clients in a digital-driven world.

## KPMG Cyber Security Services

As a leading provider and implementer of cyber security, KPMG knows how to apply leading security practices and build new ones that are fit for purpose. Our innovative approach to cyber security also includes the ways we deliver our services and clients can expect to work with extraordinary people who understand business and technology.

In addition to assessing cyber security and aligning it to business priorities, we help develop advanced approaches, monitor ongoing risks and help respond effectively to cyber incidents. We support organisations in designing and implementing robust cyber security strategies, policies, and frameworks tailored to their unique risk profiles and regulatory environments. Our teams also work closely with clients to raise workforce cyber awareness through targeted training, simulations, and behavioural change programs which help embed a culture of security across organisations.

KPMG's cyber specialists bring deep expertise across governance, risk, compliance, and emerging technologies, enabling us to deliver end-to-end solutions that are strategic and practical. No matter where our stakeholders are on their cyber security journey, KPMG helps them reach their destination with confidence and resilience.[2]

[2] https://home.kpmg/au/en/home/services/advisory/management-consulting/technology/kpmg-powered-enterprise/cyber.html

# Section 1:
# KPMG recommendations

## RECOMMENDATION 1:

Cyber security awareness campaigns should be inclusive by design, using relatable stories and tailored, jargon-free messaging to engage diverse groups. This includes partnering with trusted local organisations and embedding accessibility from the start. To have a meaningful impact, they need to be enduring and well-funded.

## RECOMMENDATION 2:

KPMG recommends tailored, accessible cyber security support for small businesses and not-for-profits through simplified tools, subsidised training, and sector-specific guidance, enabled by government and industry partnerships. Regulatory frameworks should also be scalable and suited to resource-constrained organisations.

## RECOMMENDATION 3:

KPMG supports integrating cyber security into foundational education through inclusive, tech-enabled approaches to build lifelong digital literacy and bridge the digital divide. Key actions include embedding cyber security in school curricula, expanding access to virtual learning, co-designing teacher training with experts, personalising learning with emerging technologies, and forming public-private partnerships for resources and mentorship.

## RECOMMENDATION 4:

KPMG supports Australia's adoption of a modern, enforceable data protection framework that embeds strong rights, remedies, and responsibilities. We support a further government review into mandatory support services for breach victims, and whether Australia would benefit from a unified data protection regime.

## RECOMMENDATION 5:

KPMG suggests Australia should expand its digital identity program by investing in secure, user-centric infrastructure and supporting domestic innovation to enable trusted data sharing and inclusive digital service delivery.

## RECOMMENDATION 6:

KPMG recommends strengthening Australia's cyber resilience through inclusive, cross-sector collaboration that engages government, industry, and civil society in policy development, threat response, and community uplift. This should include facilitating real-time, community-based threat sharing and promoting leading practices across sectors.

## RECOMMENDATION 7:

KPMG urges coordinated action to ensure national resilience to quantum computing. This includes transitioning critical sectors to quantum-safe cryptography through enforceable regulations, cross-sector collaboration, infrastructure modernisation, and rapid capacity-building.

## RECOMMENDATION 8:

Governments should establish a clear, risk-based regulatory framework for AI that prioritises oversight of high-risk applications while promoting innovation, aligning with international norms, strengthening data governance, and fostering trust through inclusive collaboration and strategic leadership.

## RECOMMENDATION 9:

KPMG recommends the government consider establishing a standardised, scalable national framework for managing Foreign Ownership, Control, or Influence (FOCI) risks, supported by practical tools, subsidised access to guidance for SMEs, and expert guidance.

## RECOMMENDATION 10:

KPMG suggests strengthening threat sharing programs with domestic, regional, and international partners. This should include developing a standardised approach identifying and integrating strategic partners to expand Australia's threat sharing network.

## RECOMMENDATION 11:

Australia should consider exploring initiatives to promote DNS security awareness, leading practices, and the implementation of proactive measures leveraging insights from threat sharing capabilities. Additionally, Australia should look to review government security frameworks and policies to incorporate robust DNS security considerations.

## RECOMMENDATION 12:

KPMG supports strengthening the SOCI regime by harmonising sector-specific security requirements, enhancing industry engagement, increasing priority on enforcement and compliance, and providing scalable compliance support for small businesses.

## RECOMMENDATION 13:

KPMG suggests the government develop a whole-of-government security assurance program designed to apply across all agencies and sectors. To uplift supply chain resilience, targeted support for SMEs, including grants for AI-enabled monitoring tools, and updating cyber security standards and requirements to enhance transparency, should be prioritised. Additionally, the Right Fit for Risk (RFFR) accreditation or another government-backed accreditation could apply to third parties that provide services to organisations managing IT systems or delivering managed services. Further transparency and standardised incident reporting measures could also be implemented.

## RECOMMENDATION 14:

The Australian Government should lead a national, multi-generational cyber workforce strategy that embeds age-appropriate education and career engagement from primary school onwards, supported by sustained public-private partnerships, dedicated funding, and a coordinating body to ensure long-term cyber resilience.

## RECOMMENDATION 15:

To build a resilient and innovative cyber workforce, Australia must adopt a whole-of-sector approach to embed inclusive practices and redesign pathways that support underrepresented groups from early education through to employment.

## RECOMMENDATION 16:

To support Australia's sovereign cyber security capabilities, KPMG recommends supporting sovereign capabilities through targeted support for startups and inclusive procurement reform.

## RECOMMENDATION 17:

Australia's continued commitment to the Pacific must be underpinned by a long-term vision of shared security and prosperity. KPMG recommends an approach centred on co-design, mutual collaboration, and sovereign capabilities. This will position Australia as a reliable regional supporter and a strategic partner of choice who is committed to advancing Pacific-led solutions to Pacific challenges.

# Section 2:
# KPMG insights

# KPMG insights

## Our vision for Horizon 2

Australia's cyber security landscape is evolving rapidly, demanding a coordinated, inclusive, and forward-looking approach to uplift national resilience. KPMG anticipates that Horizon 2 will be shaped by the emergence of new and developing technologies such as artificial intelligence, quantum computing, and 6G, which will significantly alter the cyber threat landscape. These technologies present both opportunities and risks, requiring agile and forward-looking policy responses. Strategic factors the Government should explore include the impact of geopolitical tensions on cyber risk, the need for harmonised regulation, and the importance of fostering a sovereign cyber industry.

KPMG's submission to the Horizon 2 Discussion Paper explores key strategic priorities to strengthen cyber awareness and maturity across sectors and communities. It highlights the importance of public engagement, support for small organisations, and inclusive education to build foundational cyber literacy. Drawing on international best practices, it outlines pathways for secure technology standards, trusted data sharing, and responsible adoption of emerging technologies. We emphasise the need to empower consumers, foster government-industry collaboration, and protect critical infrastructure.

We have identified several priority areas to help future-proof Australia's national resilience in Horizon 2. These include:

- **Public engagement and awareness:** Enhancing cyber awareness through strategic outreach and education.
- **Support for small organisations:** Helping smaller entities improve their cyber maturity.
- **Cyber education:** Promoting inclusive cyber security learning in schools.
- **Global standards:** Adopting international best practices for secure technologies.
- **Data sharing and innovation:** Enabling trusted data sharing to drive economic growth.
- **Government-industry collaboration:** Working together on secure data access and emerging tech.
- **Technology risk management:** Addressing risks from foreign influence in tech supply chains.
- **Critical infrastructure and resilience:** Strengthening national resilience through SOCI and DNS security.
- **Third Party Provider security:** Placing a concerted focus on the security of third party providers.
- **Workforce development:** Building and diversifying Australia's cyber workforce.
- **Sovereign capability:** Supporting local innovation and capability in cyber security.

Our recommendations in this submission reflect KPMG's commitment to a collaborative, forward-looking approach that integrates technical expertise, education, and strategic investment to strengthen Australia's cyber resilience.

## Shield-level focus for Horizon 2

### Shield 1: Strong businesses and citizens

#### Strengthening cyber awareness through strategic public engagement

Despite growing public attention following high-profile breaches, cyber security awareness among the general population remains low and often superficial. Australians are increasingly desensitised to data breaches, often responding with indifference, stating 'everyone has my data anyway'. This complacency stems from a lack of understanding about how exposed credentials can lead to identity theft, financial fraud, and other personal harms. To shift this mindset, government and community groups should amplify real-life stories of breach victims. Personal experiences make the risks relatable and help people connect the dots between data exposure and its consequences. Empowering people through relatable education, not fear, has the potential to rebuild public engagement and foster stronger cyber resilience.

Existing resources, such as those provided by the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC), are high quality, but their visibility and accessibility are limited. These resources are often promoted only during events such as Cyber Security Awareness Month[3], resulting in sporadic engagement and low public awareness.

To address this, cyber security messaging must adopt a sustained and universal communication strategy. Campaigns should be embedded in the media and platforms that Australians routinely engage with, including social media, community services, and mainstream news outlets. Tailored messaging is also essential, particularly for small businesses and not-for-profit organisations, as their needs differ significantly across sectors, and their capacity to interpret technical guidance is often limited.

Access to cyber resilience information is typically reactive, with individuals and organisations seeking support only after an incident has occurred. To improve preparedness, cyber security guidance should be integrated with frontline services, such as identity recovery, financial counselling, and legal aid, so that Australians know where to turn in the event of a compromise and can take preventative action before one occurs. These reforms are particularly critical for vulnerable cohorts.

Older Australians, for instance, often struggle with digital literacy and view security measures like multi-factor authentication (MFA) as barriers rather than protections. This cohort may benefit most from community-based education efforts that simplify concepts and demonstrate practical steps to stay safe online. Leveraging trusted local groups and service providers, such as accountants or banking organisations, may help bridge this gap.

Younger Australians, while more tech-savvy, are frequently unaware of the risks associated with oversharing personal information online. Early education in schools, combined with engaging social media campaigns, is crucial to instilling foundational cyber hygiene habits. Similarly, parents often lack awareness of digital threats, making it essential for schools to include cyber safety messaging in newsletters and parent information sessions.

Individuals with a disability may encounter accessibility challenges with mainstream cyber education materials, which are often not designed with inclusive formats such as screen reader compatibility, plain language, or visual aids. Cyber security messaging must be adapted to meet diverse cognitive and physical needs, ensuring that protective measures like MFA or secure browsing practices are both usable and understandable. Partnering with disability advocacy organisations and leveraging assistive technologies can help bridge this gap.

First Nations communities may face cultural, linguistic, and geographic barriers that limit their engagement with conventional cyber awareness campaigns. For communities living in remote locations there may be limited digital infrastructure, and mainstream messaging may not resonate due to cultural disconnects. Co-designing cyber education initiatives with Indigenous organisations and community leaders is critical. This includes using culturally appropriate narratives, delivering content in local languages, and embedding cyber safety into broader community wellbeing programs.

Government and industry must work with local community groups, health services, and educational institutions to deliver cyber awareness in familiar, supportive environments. Campaigns should avoid technical jargon and instead focus on relatable stories that demonstrate the real-life impacts of cyber threats, such as scams targeting pensioners or data breaches affecting community services.

To be effective, cyber security awareness must be inclusive by design, not retrofitted. This means embedding accessibility, cultural relevance, and community engagement into every stage of campaign development and delivery. By doing so, Australia can ensure that no group is left behind in the national effort to build cyber resilience.

## RECOMMENDATION 1:

Cyber security awareness campaigns should be inclusive by design, using relatable stories and tailored, jargon-free messaging to engage diverse groups. This includes partnering with trusted local organisations and embedding accessibility from the start. To have a meaningful impact, they need to be enduring and well-funded.

[3] Cyber Security Awareness Month 2024 | Cyber.gov.au

### Empowering small organisations to uplift their cyber security maturity

Small and medium enterprises (SMEs) and not-for-profits (NFPs) face significant challenges in achieving cyber security maturity due to limited resources, lack of dedicated time to cyber security maturity building, and a lack of tailored support for a business's unique threat environment.

For small businesses, cyber security responsibility often rests with one person, or a very small team, who is already managing multiple core functions such as financial oversight, day-to-day operations, customer service, and marketing. This limited capacity means cyber security is frequently deprioritised, not due to lack of concern, but because of competing demands and resource constraints. Without dedicated cyber expertise, these individuals may struggle to assess risks, implement safeguards, or respond effectively to incidents. This highlights the need for simplified, accessible tools and guidance tailored to small business contexts, as well as support from government and industry to embed cyber resilience into routine business practices.

Not-for-profit organisations face unique challenges in achieving cyber security maturity, largely due to limited funding, lean staffing, and a mission-driven focus that prioritises service delivery over technical infrastructure. Cyber security responsibilities often fall to generalist staff or volunteers who lack formal training and are already stretched across multiple roles. Additionally, NFPs may underestimate their risk exposure, assuming they are less likely to be targeted than commercial entities. To address these barriers, tailored support is needed, such as subsidised training, simplified tools, and sector-specific guidance, to help NFPs build resilience without diverting focus from their core mission.

SMEs and not-for-profit organisations often struggle to absorb the financial burden of cyber security uplift programs, as their limited budgets are typically directed toward core operations. To overcome these constraints, targeted financial assistance and tailored educational initiatives are essential. Government and industry partnerships can play a pivotal role by co-developing or funding sector-specific resources that are practical and accessible. Embedding cyber security requirements into foundational business processes, such as payroll, compliance, and risk management, can help normalise cyber resilience as a standard part of operations.

Outsourcing IT services, while common among SMEs, can create a false sense of security. Many assume that risk is transferred to providers, when accountability remains with the business. Clearer guidance on roles, responsibilities, and risk ownership is needed. Practical support measures, such as curated directories of trusted providers and simplified procurement pathways, can help small organisations navigate the complex cyber landscape. Additionally, regulatory frameworks should be inclusive and scalable, ensuring minimal standards are met without placing undue pressure on resource-constrained organisations.

## RECOMMENDATION 2:

KPMG recommends tailored, accessible cyber security support for small businesses and not-for-profits through simplified tools, subsidised training, and sector-specific guidance, enabled by government and industry partnerships. Regulatory frameworks should also be scalable and suited to resource-constrained organisations.

### Advancing inclusive cyber security education in Australian schools

Australia's education system continues to face a digital divide, with unequal access to technology and varying levels of digital literacy hindering equitable learning outcomes, particularly in STEM. These disparities, shaped by cultural, demographic, and socioeconomic factors, often force schools to rely on offline materials. To address this, teaching resources must be inclusive and adaptable to a wide range of digital competencies.

Cyber security awareness is a vital part of digital literacy, especially as students increasingly engage with online platforms. Initiatives such as KPMG's Global Cyber Day[4] have shown success in raising awareness among students, teachers, and parents through engaging, real-world learning experiences. Building on these efforts requires collaboration between educators and cyber professionals to scale impactful programs.

Key opportunities include:

- Embedding cyber security into school curricula across year levels.

[4] Global Cyber Day – KPMG

- Expanding access to virtual environments that simulate cyber threats and safe practices.
- Co-designing teacher training with technical experts to build confidence.
- Leveraging emerging technologies to personalise learning and identify gaps.
- Establishing public-private partnerships to provide resources, mentorship, and infrastructure.

A collaborative, cross-sector approach is essential to ensure educational content remains relevant and responsive to evolving cyber threats. By integrating cyber security into foundational learning, Australia can equip students with the skills and confidence to navigate an increasingly digital world.

## RECOMMENDATION 3:

KPMG supports integrating cyber security into foundational education through inclusive, tech-enabled approaches to build lifelong digital literacy and bridge the digital divide. Key actions include embedding cyber security in school curricula, expanding access to virtual learning, co-designing teacher training with experts, personalising learning with emerging technologies, and forming public-private partnerships for resources and mentorship.

## Shield 2: Safe technology

### International best practices for secure technology standards and frameworks

Australia's cyber security landscape is evolving rapidly, yet our legislative framework for data protection is considered, by some, as being behind global standards. Australia could benefit from a more comprehensive and enforceable data protection regime that adequately safeguards personal information, enables the safe transfer and use of personal information for the benefit of individuals and the community, and supports victims of cybercrime.

The Australian Government's Cyber Security Strategy and Horizon 2 Discussion Paper outline commendable initiatives to uplift national cyber resilience. However, to fully realise the Strategy's vision of making Australia a world leader in cyber security by 2030, future reform could address gaps in data protection and victim support. This should include:

**1. Enhance support services for breach victims**

Cyber incidents, particularly those involving identity theft, impose significant emotional, financial, and administrative burdens on individuals. The Horizon 2 Discussion Paper acknowledges the growing demand for support services and the need for scalable infrastructure. KPMG considers that a national framework for victim support should be assessed, including case management, identity recovery assistance, and mental health services, with clear communication protocols to ensure accessibility for vulnerable cohorts.

**2. A review of penalties for organisations that fail to protect personal data**

The current regulatory environment could improve deterrents for negligent data handling. In addition, as outlined in Shield 1 and Shield 4 of the Strategy, harmonising and simplifying cyber regulation is essential.

**3. A modern, enforceable data protection framework**

The Strategy's commitment to protecting critical datasets and promoting secure technology is commendable. Policy makers could consider a unified data protection framework that consolidates existing obligations under the Privacy Act, Security of Critical Infrastructure (SOCI) Act, and other sectoral regulations. The framework could include mandatory breach notification, data minimisation principles and enforceable rights for individuals.

## RECOMMENDATION 4:

KPMG supports Australia's adoption of a modern, enforceable data protection framework that embeds strong rights, remedies, and responsibilities. We support a further government review into mandatory support services for breach victims, and whether Australia would benefit from a unified data protection regime.

## Achieving trusted data sharing to boost innovation and economic prosperity

Trusted digital identity systems are foundational to secure data sharing and digital service delivery. International exemplars such as Singapore's Singpass MyInfo[5] and Estonia's e-Identity[6] demonstrate how well-designed identity frameworks can enable seamless, secure access to both public and private sector services, while fostering public trust and economic growth.

Singapore's MyInfo provides residents with a single, secure login for a wide range of services, incorporating biometric authentication, streamlining digital transactions involving personal data. Its integration across government and commercial platforms streamlines user experience and strengthens identity assurance. Estonia's system, in place for over two decades, mandates digital IDs for citizens and offers e-Residency for non-citizens. It underpins nearly all aspects of Estonia's digital society, from voting and banking to healthcare and business registration.

Both models succeed because they are:

- **Universal and interoperable**, enabling consistent access across sectors;
- **Secure by design**, incorporating advanced authentication and fraud prevention;
- **User-centric**, with intuitive interfaces and minimal friction; and
- **Supported by strong legislative and institutional frameworks**, ensuring privacy and accountability.

An expanded Australian digital ID program presents a significant opportunity to replicate these benefits. However, to fully realise the economic and innovation potential of trusted data sharing, further investment is needed, not only in identity infrastructure, but in the broader digital ecosystem.

Trusted data sharing is not just a technical challenge, it is a strategic enabler of national productivity, competitiveness, and resilience. By learning from global best practice and investing in local innovation, Australia can build a digital economy that is both secure and prosperous.

## RECOMMENDATION 5:

KPMG suggests Australia should expand its digital identity program by investing in secure, user-centric infrastructure and supporting domestic innovation to enable trusted data sharing and inclusive digital service delivery.

## Government-industry collaboration on data access and secure sharing

Meaningful collaboration between government, industry, and civil society is just as vital to Australia's cyber resilience as strong regulation and technical expertise. Engagement between government and industry has improved markedly in recent years, with initiatives such as the Executive Cyber Council helping to foster genuine co-leadership on national cyber priorities. This momentum must be sustained and expanded to ensure that policy development reflects the diversity of Australia's economic landscape.

To strengthen this collaboration, government should broaden its consultation efforts to include a wider range of enterprise sizes and sectors, particularly small businesses and not-for-profit organisations. Cyber-focused not-for-profits also play a critical role in community uplift, education, and workforce development. Strategic partnerships with these organisations through grants, internships, and pilot programs can amplify the reach and impact of national cyber initiatives.

Industry-to-industry collaboration is equally vital. The interconnectivity of sectors means that cyber threats often span multiple domains, including scams, fraud, and identity crime. Addressing these challenges requires a shared, integrated view of the threat environment. Organisations should be encouraged to include a wide range of stakeholders in cyber wargaming and incident response exercises, fostering a collective understanding of roles and responsibilities during crises.

No single entity can manage the full spectrum of cyber threats alone. A community-based approach to incident response, where businesses, regulators, and service providers coordinate in real time, is essential to mitigating harm and restoring trust. Government can support this by facilitating cross-sectoral threat sharing, promoting best practice, and ensuring that all stakeholders have access to timely and actionable intelligence.

[5] Myinfo | Singapore Government Developer Portal
[6] ID-card - e-Estonia

## RECOMMENDATION 6:

KPMG recommends strengthening Australia's cyber resilience through inclusive, cross-sector collaboration that engages government, industry, and civil society in policy development, threat response, and community uplift. This should include facilitating real-time, community-based threat sharing and promoting leading practices across sectors.

### Guidance for safe and responsible uptake of critical and emerging technologies

#### *Safe adoption of quantum*

To support the safe and responsible uptake of critical and emerging technologies, particularly quantum computing, governments must take a proactive, multi-pronged approach that combines regulation, collaboration, infrastructure support, and capacity building.

First, governments should consider clear and enforceable regulatory frameworks that mandate the transition to quantum-safe cryptography across critical sectors. This includes updating cyber security standards, procurement policies, and compliance requirements to reflect the evolving threat landscape. Examples such as the U.S. Quantum Computing Cybersecurity Preparedness Act,[7] the Cyber Security Agency of Singapore (CSA) Cyber Essentials or Cyber Trust marks,[8] and the Australian Signals Directorate's revised guidelines demonstrate how national mandates can drive industry-wide readiness. These frameworks should be harmonised across jurisdictions to ensure consistency and avoid fragmented adoption that could weaken interconnected systems.

Second, governments can play an important role in fostering industry collaboration and knowledge sharing. By supporting initiatives like the Quantum Safe Cryptography Working Group led by the Emerging Payments Association Asia (EPAA),[9] governments can help convene stakeholders across banking, fintech, infrastructure, and regulatory bodies to co-develop roadmaps, standards, and interoperability frameworks. Such platforms enable coordinated action, promote crypto agility, and ensure that diverse business models and jurisdictions are accounted for in the transition to quantum resilience.

Third, governments should provide guidance and incentives for infrastructure modernisation and cryptographic agility. This includes encouraging the adoption of Post-Quantum Cryptography (PQC) and other quantum-resilient technologies such as Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNGs). By supporting simplification of legacy systems, updating data retention policies, and enabling hybrid cryptographic approaches, governments can help organisations reduce implementation risks and improve long-term resilience.

Finally, building awareness and capacity across the ecosystem is essential. Many organisations lack visibility into how and where their data is encrypted, which magnifies the challenge of quantum resilience. Governments should invest in education campaigns, training programs, and technical support to help organisations develop cryptographic bills of materials (CBOMs), assess risk profiles, and coordinate cross-functional teams. These efforts should extend beyond IT departments to include legal, procurement, compliance, and executive leadership, fostering a whole-of-organisation approach to cyber security.

## RECOMMENDATION 7:

KPMG urges coordinated action to ensure national resilience to quantum computing. This includes transitioning critical sectors to quantum-safe cryptography through enforceable regulations, cross-sector collaboration, infrastructure modernisation, and rapid capacity-building.

#### *Safe and responsible uptake of Artificial Intelligence*

[7] H.R.7535 - 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act | Congress.gov | Library of Congress
[8] Certification for the Cyber Essentials Mark | Cyber Security Agency of Singapore
[9] Emerging Payments Association Asia announces new work group to encourage the adoption of quantum-safe cryptography in the banking industry - 25 April 2024

Australians are experiencing a range of benefits from the use of AI. Individuals are experiencing improved efficiency and effectiveness, enhanced accessibility to information and greater personalisation of content they interact with online. KPMG, for example, has worked to integrate AI into its operational functions, making it a familiar tool used to improve efficiency and quality of outputs.

However, these benefits are coupled with risks that need to be considered. One of these risks associated with AI is its potential to generate misinformation. This has the potential to significantly erode public trust in online content and poses a risk to Australia's national security and social cohesion. As detailed in the University of Melbourne and KPMG 2025 global study, 'trust, attitudes and use of artificial intelligence', people are looking to news and social media companies to implement stronger fact-checking processes.[10] There is a need to combat AI-generated misinformation and establish methods to allow individuals to detect when content is AI-generated. The proliferation of AI-generated misinformation also poses a threat to democratic processes, with 64% of respondents expressing concern about election manipulation.[11]

To support the safe and responsible uptake of AI, the Commonwealth can play a pivotal role by providing clear, strategic, and proportionate guidance. A foundational step is to ensure Australia's regulatory environment contains sufficient guardrails around high-risk AI. There is a strong global mandate for regulation, with 70% of respondents to the University of Melbourne and KPMG 2025 global study supporting the need for AI laws. Only 43% of respondents believe the current regulations are adequate.[12] International cooperation is also essential, recognising that AI systems often operate across borders and are developed by multinational entities.

Regulatory efforts should be aligned with existing laws and international norms, integrating AI governance with privacy, consumer protection, and cybersecurity frameworks, and ensuring interoperability with global standards like the EU AI Act[13] and OECD AI principles[14]. To foster innovation, especially among SMEs, regulation must be clear, scalable, and proportionate, supported by initiatives like the National AI Centre that offer funding, training, and shared infrastructure. Further, governments should strengthen data governance and access, learning from international models to improve availability of high-quality datasets while safeguarding privacy. Building a trusted environment is essential, requiring enforceable regulation, public sector leadership, inclusive collaboration, and capability-building across the economy. In addition, the University of Melbourne and KPMG 2025 global study found that 83% of people are unaware of any laws governing AI in their country.[15] This underscores the need for awareness campaigns and training programs to empower citizens with knowledge of their rights and responsibilities.

The Commonwealth should act decisively to balance the benefits of AI with its risks. This requires a coordinated approach that includes regulation, education, international collaboration, and support for responsible innovation.

## RECOMMENDATION 8:

Governments should establish a clear, risk-based regulatory framework for AI that prioritises oversight of high-risk applications while promoting innovation, aligning with international norms, strengthening data governance, and fostering trust through inclusive collaboration and strategic leadership.

### Managing foreign ownership, control, or influence risks in technology vendors

As Australia deepens its reliance on digital infrastructure and foreign-sourced technologies, the need for a robust and standardised approach to managing foreign ownership, control, or influence (FOCI) risks has become increasingly urgent. While the Department of Home Affairs has provided initial guidance on conducting FOCI risk assessments[16], current frameworks are limited in scope and operational utility. Existing materials, including the sample questionnaire, offer a compliance-oriented checklist but fall short of enabling meaningful risk management.

[10] Trust, attitudes and use of artificial intelligence: A global study 2025
[11] Trust, attitudes and use of artificial intelligence: A global study 2025
[12] Trust, attitudes and use of artificial intelligence: A global study 2025
[13] Regulation - EU - 2024/1689 - EN - EUR-Lex
[14] AI principles | OECD
[15] Trust, attitudes and use of artificial intelligence: A global study 2025
[16] Foreign Ownership, Control or Influence Risk Assessment Guidance

Critical gaps remain in the assessment of FOCI risks. For example, the guidance does not adequately address scenarios where foreign contracts or agreements constitute a significant portion of an entity's revenue, nor does it consider the influence of critical suppliers embedded within the technology supply chain. Furthermore, there is no standardised classification of jurisdictional risk beyond the Five Eyes alliance, leaving ambiguity around what constitutes low, medium, or high-risk foreign influence.

The reliance on open-source intelligence (OSINT) as the primary assessment tool is also problematic. OSINT data is often incomplete, expensive to analyse, and inaccessible to SMEs. Commercial software capable of conducting comprehensive FOCI assessments is prohibitively costly, and many organisations lack the internal capability to interpret the results. Upskilling across industry is essential, as many practitioners may not recognise nuanced indicators of foreign influence or control.

To address these challenges, the Government should consider the following actions:

- **Develop a standardised national framework for FOCI risk assessment**, including clear definitions of jurisdictional risk levels, guidance on evaluating contractual, financial, and supply chain dependencies, and example case studies demonstrating how the guidance can be applied.
- **Expand and refine the existing Home Affairs guidance**, incorporating practical tools and case studies that reflect real-world complexities. This should include practical tools such as sample contract clauses.
- **Subsidise access to FOCI assessment tools and training for SMEs**, ensuring that all entities, regardless of size, can participate in secure procurement and risk mitigation practices.
- **Establish a centralised advisory service or helpdesk**, enabling organisations to seek expert support in navigating FOCI-related concerns.

A consistent and scalable approach to managing FOCI risks will strengthen Australia's cyber resilience, protect critical infrastructure, and ensure that technology procurement decisions are aligned with national security interests.

## RECOMMENDATION 9:

KPMG recommends the government consider establishing a standardised, scalable national framework for managing Foreign Ownership, Control, or Influence (FOCI) risks, supported by practical tools, subsidised access to guidance for SMEs, and expert guidance.

## Shield 3: World-class threat sharing and blocking

### Resilience through collaboration

The contemporary digital landscape is characterised by increasingly sophisticated and frequent cyber threats, by foreign state actors, extremist groups, malicious individuals. These entities threaten the economic, social and cultural prosperity of Australia and its strategic partners. Developing threat intelligence sharing capabilities with both domestic and international partners is now a mandatory matter of national security, ensuring nations are informed, responsive and proactively investing in the resilience of local government, businesses and citizens.

Australian should continue to promote programs such as ASD's Cyber Threat Intelligence Sharing (CTIS)[17], ensuring open two-way sharing between government and industry partners. Programs like the inclusion of a freely available Microsoft plugin for the CTIS, represent practical steps to further the adoption of the service by small, medium and large organisations which is an important factor in strengthening initiative and contributes to the collective benefit.

Apart from existing collaboration with Five Eyes (FVEY) countries, Australia's position in the Pacific region as a trusted cyber leader also provides opportunities for expanding its threat intelligence network to incorporate continuous and valuable insights from regional neighbours. The Pacific Cyber Security Operational Network (PaCSON)[18] represents one such avenue for exploration on enabling mutually beneficial collaboration with Australia's "Pacific Family". Diversity in partners provides Australia with a

[17] Join the Cyber Threat Intelligence Sharing service through Sentinel | Cyber.gov.au
[18] About us | Pacific Cyber Security Operational Network (PaCSON)

comprehensive and accurate perspective of the global threat landscape, informing the nation how best to secure its strategic interests.

## RECOMMENDATION 10:

KPMG suggests strengthening threat sharing programs with domestic, regional, and international partners. This should include developing a standardised approach to identifying and integrating strategic partners to expand Australia's threat sharing network.

### Securing DNS

A key enabler of contemporary threats is Domain Name Services (DNS) as gateway to target digitised services and infrastructure. DNS-enabled attacks such as ransomware, phishing and data breaches are only escalating in sophistication as advanced persistent threats (APT) - criminal groups, extremist groups, and foreign state actors - converge on cyber attacks to carry out their agendas.

An identified gap in DNS security is the absence of capability to proactively identify and mitigate sophisticated DNS-based threats. Current DNS security practices focus on passive and preventative measures - such as Domain Name System Security Extensions (DNSSEC), DNS over Hypertext Transfer Protocol (HTTP), and DNS over Transport Layer Security (TLS) - which provide assurance over individual packets. As a globally recognised security framework, the National Institute of Standards and Technology (NIST) Cyber Security Framework recently revised its secure DNS deployment guidance (SP 800-81) to incorporate proactive and dynamic DNS measures, including mandating the use of technologies such as protective domain name services (PDNS) to meet sophisticated threats. As such it is imperative that Australia recognises the need for proactive DNS security measures (such as the Australian Protective DNS) to complement current practices in a scalable, sustainable and fit-for-purpose manner.

## RECOMMENDATION 11:

Australia should consider exploring initiatives to promote DNS security awareness, leading practices, and the implementation of proactive measures leveraging insights from threat sharing capabilities. Additionally, Australia should look to review government security frameworks and policies to incorporate robust DNS security considerations.

## Shield 4: Protected critical infrastructure

### Optimising SOCI for national cyber resilience

The Security of Critical Infrastructure Act (SOCI Act) is the cornerstone of Australia's legislative framework to safeguard essential services across eleven critical sectors. The SOCI Act addresses the growing complexity and interdependence of Australia's critical infrastructure systems, taking an all-hazards approach to enhance resilience across all sectors. Recent amendments have expanded the scope of the SOCI regime to address evolving security risks and enhance resilience outcomes.

To enable the SOCI regime to more effectively meet its strategic objectives, there are opportunities to further harmonise and streamline legislation, consolidating overlapping sector-specific requirements. Steps have been taken in this direction, such as through the integration of key security obligations from Part 14 of the *Telecommunications Act 1997* into SOCI via the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024*, however there is scope for other sector-specific security requirements to be further aligned with the SOCI regime. Harmonising security requirements, reporting processes, and standards will work to reduce regulatory burden and duplication across critical infrastructure sectors while also enhancing the SOCI regime's ability to address sector-specific risks. Any such harmonisation of security requirements should be developed and conducted in close collaboration and consultation with the regulatory bodies of each critical infrastructure sector, and the broader industry that changes would impact directly or indirectly.

Beyond legislative alignment, the effectiveness of the SOCI regime depends on proactive engagement with industry. The Critical Infrastructure Security Centre (CISC) plays a critical role in setting the tone and driving a strong compliance and security culture throughout SOCI regulated entities. For example, if

CISC is proactive in its push-communications with industry, and if it takes a thorough, detailed, and risk-based approach to audits on critical infrastructure owners and operators, industry is more likely to engage proactively with their SOCI obligations, and treat SOCI as more than a 'tick the box' compliance exercise. To strengthen this outcome, the Department of Home Affairs should adopt a more proactive compliance and enforcement posture, building on reforms to the SOCI regime to include expanded audit requirements and forward-leaning compliance measures. Such an approach would provide greater assurance that obligations are met consistently across sectors, reinforce the national priority placed on critical infrastructure resilience, and ensure that non-compliance is promptly and effectively addressed in partnership with industry. Additionally, building a community of practice through forums such as the Trusted Information Sharing Network (TISN), sharing positive case studies, and encouraging cross-sector collaboration will help foster a culture of continuous improvement and proactive collaboration. Importantly, industry must be incentivised to go beyond minimum compliance, as the security threat landscape is evolving faster than regulatory updates can keep pace.

The market failure the SOCI Act amendments sought to correct may be better addressed by evolving the CISC's compliance and enforcement posture. The CISC's collaborative approach and focus on security uplift has been entirely appropriate to date, and indeed, should continue to help mature the collective awareness of security and resilience. However, there is a risk of an increasing minimum compliance-based approach to SOCI, which will not meet the intent of the reforms. In an environment of cost and price competitiveness, Boards and Executive Management teams will prioritise the matters on which they are measured and judged. Increased priority on compliance and enforcement ahead of another major incident will drive the desired priority on security and resilience, while complementing the operational-level engagement through the TISN.

Tailored support and guidance should also be given to smaller businesses who are captured under the SOCI regime, as these entities often face significant challenges in meeting compliance obligations due to limited resources, expertise, and capacity. Unlike larger organisations, these smaller businesses often lack the resources to fully or rapidly implement complex regulatory requirements, which can place undue strain on their operations. Without tailored support, this can lead to inconsistent compliance and increased vulnerability across critical infrastructure sectors. To ensure the SOCI regime is inclusive and effective, the Commonwealth should consider scalable compliance pathways and provide practical guidance for small businesses to enable them to contribute meaningfully to national resilience without being overwhelmed due to regulatory burden.

## RECOMMENDATION 12:

KPMG supports strengthening the SOCI regime by harmonising sector-specific security requirements, enhancing industry engagement, increasing priority on enforcement and compliance, and providing scalable compliance support for small businesses.

### Embedding security across the economy

Australian Government security requirements are increasingly being adopted in the private sector through programs such as the Defence Industry Security Program (DISP), which sets clear security expectations for Defence industry suppliers, and the Hosting Certification Framework (HCF), which mandates alignment with key Protective Security Policy Framework (PSPF) requirements for data centre and cloud service providers hosting sensitive Commonwealth data. While these frameworks have proven effective in raising baseline standards within specific sectors, their scope remains limited to particular domains, leaving gaps in consistency across broader Government procurement and engagement.

To address this, the Commonwealth should develop a whole-of-government security assurance program, modelled on the intent of DISP but designed to apply across all agencies and sectors. Such a program would establish unified, scalable security expectations for any organisation seeking to engage with the Commonwealth, regardless of the department or service area. This would streamline compliance and reduce some regulatory duplication while ensuring all suppliers meet robust and consistent security standards. By embedding this approach into procurement processes, the Commonwealth can uplift national resilience, foster trust in public-private collaboration, and ensure that security is treated as a foundational requirement across the Commonwealth.

With an increasing number of cyber incidents being enabled by vulnerabilities in third-party suppliers, uplifting supply chain security should be a concerted priority for Horizon 2. Recent cyber incidents have highlighted how vulnerabilities in a single supplier can lead to the compromise of sensitive data and

disruption to the delivery of key services. No sector is immune to third party and supply chain risk, which is magnified by the small and medium businesses which often make up the bulk of organisations' supply chains and lack the resources and technical expertise to embed robust security controls. Support for these suppliers is critical to effectively uplift the cyber resilience of the Australian economy.

There are a number of options that could be considered to help address the national vulnerability associated with third party providers. AI-enabled solutions can drive greater real-time visibility of suppliers' security exposure, and can continuously monitor and analyse vast amounts of data beyond what manual audits or periodic reviews can achieve. Buyers could insist on using these tools, equally, vendors could consider providing improved transparency to clients via such real-time insights. However, until these solutions become more mainstream and accessible, the Commonwealth could consider providing practical help for SMEs embedded in supply chains by offering grants and incentives for these tools, making them more accessible while simultaneously updating key cyber security standards to require more robust and proactive continuous monitoring of supplier security to keep pace with evolving security threats. Targeted support for suppliers while comprehensively uplifting supply chain security standards will ensure that security expectations are clear and achievable, and secure Australia's economy while fostering accessible and equitable access to innovative solutions.

More specifically, the Right Fit for Risk (RFFR) accreditation, currently used for government-facing systems, could be expanded to include third parties that provide services to organisations managing IT systems or delivering managed services. This would ensure that vendors supporting regulated sectors are held to the same rigorous standards as those directly interfacing with government systems. The accreditation system could also be a government-backed certification framework that is mandatory for vendors operating in regulated sectors. This would create a consistent benchmark for cybersecurity maturity and reduce ambiguity in vendor selection. Take-up could also be encouraged by insurers recognising certifications and offering premium incentives for certified vendors, driving broader adoption of best practices.

Lastly, trust must be earned through transparency. Vendors could be required to disclose their security posture, including patching cadence, incident response capabilities, and control maturity. Contracts should include audit and monitoring rights, allowing organisations to verify compliance and detect issues in real time. Additionally, incident reporting obligations could be standardised, ensuring timely disclosure of breaches or vulnerabilities that could impact client data or systems.

### RECOMMENDATION 13:

KPMG suggests the government develop a whole-of-government security assurance program designed to apply across all agencies and sectors. To uplift supply chain resilience, targeted support for SMEs, including grants for AI-enabled monitoring tools, and updating cyber security standards and requirements to enhance transparency, should be prioritised. Additionally, the Right Fit for Risk (RFFR) accreditation or another government-backed accreditation could apply to third parties that provide services to organisations managing IT systems or delivering managed services. Further transparency and standardised incident reporting measures could also be implemented.

## Shield 5: Sovereign capabilities

### A strategic approach to building Australia's cyber workforce

To ensure Australia's long-term cyber resilience, the government must take a proactive and strategic role in cultivating a robust cyber workforce. This involves a multi-generational approach that begins with early education and sustained career engagement. The government can show leadership and accountability at Ministerial and Senior Official level will drive meaningful progress.

The Australian government should craft such a strategy, uplifting the base level of cyber awareness, understanding and skill from the earliest possible age, thus sparking and fanning an interest that will drive the future cyber workforce's numbers and competence. Research has shown that embedding age-appropriate cyber study early on will yield substantial results. Moreover, evidence shows that career preferences begin forming as early as primary school, yet presently, cyber-related guidance is typically introduced too late, often in Years 11 and 12, after many students have already ruled out STEM pathways. To address this, it is recommended to embed age-appropriate cyber career engagement from Years 5 to 8.

Workforce-related programs should follow and flow smoothly with a deliberate education strategy and campaign. This would include dedicated grants and scholarships and job placements support, among

other opportunities. Importantly, the public-private partnership must be sustained and fuelled in a bid to cater to the nation's bleeding edge cyber needs at all times, while engaging the right talent. A policy and regulatory support framework would be required to enable said collaboration and set the overarching strategy up for success. This work would benefit greatly from a dedicated body established specifically for the delivery of the strategy, with a committed team akin to the National Initiative for Cyber Education (NICE) in the United States.

## RECOMMENDATION 14:

The Australian Government should lead a national, multi-generational cyber workforce strategy that embeds age-appropriate education and career engagement from primary school onwards, supported by sustained public-private partnerships, dedicated funding, and a coordinating body to ensure long-term cyber resilience.

### Diversifying Australia's cyber security workforce

Australia's cyber security workforce continues to face significant diversity gaps, particularly among women, First Nations peoples, neurodivergent individuals, and people with disabilities. Women make up just 17 percent of the cyber workforce,[19] with barriers rooted in early gender socialisation, limited role models, and workplace bias. First Nations Australians are similarly underrepresented, comprising only 0.5 percent of the STEM-qualified workforce.[20] Neurodivergent individuals and people with disabilities also encounter systemic obstacles, including inaccessible environments and limited tailored support, despite possessing strengths well-suited to cyber roles.

Addressing these disparities is not only a matter of equity, but also essential for building a resilient and innovative cyber workforce. A whole-of-sector approach is needed, involving government, industry, and education to embed inclusive practices, redesign pathways, and support diverse talent from early education through to employment. By tackling these barriers, Australia can unlock a broader talent pool and strengthen its cyber capabilities for the future.

## RECOMMENDATION 15:

To build a resilient and innovative cyber workforce, Australia must adopt a whole-of-sector approach to embed inclusive practices and redesign pathways that support underrepresented groups from early education through to employment.

### Driving sovereign capabilities through targeted support

To effectively drive innovation that supports Australia's strategic, economic, and community interests, collaboration between industry and government must be structured, targeted, and responsive to market realities. Through KPMG's engagements with Australian Chief Information Security Officers, we understand that many Australian startups relocate offshore, particularly to the US, due to larger investment pools, access to broader markets, and a more risk-tolerant investment culture. To retain and grow sovereign capability, the Australian government should support startups through targeted funding, tax breaks, streamlined procurement pathways, and incentives to procure Australian capabilities while avoiding protectionist policies.

To help small startups build reputability and gain traction in the market, the Commonwealth should prioritise their inclusion in proof-of-concept deployments within smaller agencies. This approach would allow Australian startups to demonstrate the value and effectiveness of their products and services in real-world settings. Complementing this, a formal assessment framework should be established to certify startups that meet defined standards, helping buyers identify credible local providers and reducing perceived risk. While current government support focuses on helping companies' market overseas, funding should be redirected to promote Australian solutions domestically, improving visibility and uptake. This will simplify the evaluation of product security credentials and compliance. Together, these measures will help build trust in sovereign

[19] Women critical to future of Australia's cyber security: report - RMIT University
[20] STEM-Equity-Monitor-data-summary-report-2024.pdf

solutions, support local innovation, and ensure Australian cyber capabilities are recognised and adopted at home.

A perception that certain country cyber products are superior often leads to their default procurement, overshadowing capable Australian alternatives. This bias, combined with a limited range of service offerings from local startups, highlights the need for clearer guidance on where sovereign capability should be developed. To address this, the Sovereign Capability Workstream of the Executive Cyber Council is delivering a national framework to define 'sovereign capability' and assess it against international standards. To maximise the impact of this work, the Government should formally adopt and promote this framework across relevant agencies, and use it to guide targeted investment, procurement decisions, and policy development.

Australia's current tendering process additionally presents significant challenges for cyber startups, often excluding them from opportunities that are critical for their growth. Complex procurement processes, limited panel openings, and stringent requirements can be prohibitive for small players. Private sector tenders are often complex for startups to navigate, making it difficult for them to clearly articulate their value proposition or build relationships with key decision-makers, and require small suppliers to obtain costly accreditations. To address these barriers, the Commonwealth should introduce tender preferences for Australian products and services, including minimum local procurement thresholds across State and Federal Government departments and agencies. Establishing a Supply Nation-like initiative for small cyber businesses would also help them secure contracts and gain visibility. Further support could additionally include bid templates and guidance materials for Government procurements, and subsidies for certification costs to improve eligibility. Encouragingly, the Australian Cyber Exchange 2025 featured an agenda item where industry discussed procurement processes with cyber providers, helping startups better understand how buyers go to market and how to position themselves effectively.

## RECOMMENDATION 16:

To support Australia's sovereign cyber security capabilities, KPMG recommends supporting sovereign capabilities through targeted support for startups and inclusive procurement reform.

## Shield 6: Resilient region and global leadership

### Aligning Australia with the Pacific

Reinforcing its commitment to Pacific sovereignty and resiliency, Australia should continue to position itself as a guiding and supporting partner, allowing the Pacific to develop sovereign capabilities rather than providing point in time and externally provided support. This involves ensuring programs in the Pacific align with and honour regional initiatives such as the Blue Pacific Continent Declaration, Lagatoi Declaration, and Memorandum of Understanding (MoUs). Such political agreements should serve as strategic reference points to ensure that Australia's efforts align with Pacific-led priorities, reinforcing respect for regional autonomy and shared governance.

Through engagements with Pacific governments, KPMG recognises capacity building remains a core necessity for Pacific nations. Uplift in the region is also critical to Australia's strategic interests. Australia should continue to invest in capacity building, however, sustainable and long-term impact stems from ensuring this capacity is, wherever possible, sovereign owned. This entails the provision of tangible resources, skills transfer, and operational support that ultimately enables local institutions to independently manage their development and security challenges. The emphasis should be on action-oriented partnerships that translate into real capabilities on the ground.

Another core challenge within the Pacific is visibility of the contemporary threat landscape. Australia and its Pacific neighbours face mutual threats from malicious cyber actors, whose activities transcend borders. This shared vulnerability underscores the need for a collaborative defence posture. Pacific nations are advancing through the establishment of Security Operations Centres (SOCs) and Computer Emergency Response Teams (CERTs). However, these emerging capabilities require sustained support to reach full maturity. Australia should assist in developing frameworks for routine cyber health checks, situational threat awareness, and regional intelligence sharing. As these capabilities are established, this will allow for mature collaborative activities to be undertaken such as joint threat analysis, coordinated response exercises, and

secure communication platforms enhancing regional cyber resilience but also deepening trust and cooperation. A proactive stance will empower Pacific Countries and Australia to identify and counter mutual threats before they escalate, ensuring a resilient and prosperous region.

## RECOMMENDATION 17:

Australia's continued commitment to the Pacific must be underpinned by a long-term vision of shared security and prosperity. KPMG recommends an approach centred on co-design, mutual collaboration, and sovereign capabilities. This will position Australia as a reliable regional supporter and a strategic partner of choice who is committed to advancing Pacific-led solutions to Pacific challenges.

## Key authors and contacts

[redacted]

**KPMG.com.au**