WHITE PAPER

Public Sector Insights: Setting the 2026 Audit Committee Agenda

Key focus areas in the year ahead for the Australian government

BY RICH TURLEY, ELLY MADDY AND WILL HUNT

protiviti®
Global Business Consulting

2026 promises to be another year of increasing demands for audit committee members in Australian federal and state governments. The seven topics we have highlighted for this year's audit committee agenda reflect a growing array of responsibilities that may extend beyond traditional boundaries. As oversight expectations continue to evolve, many audit committees are being called upon to engage with broader enterprise risks and governance matters. Risks, spanning cyber, AI, and talent, among others, are also becoming increasingly interdependent, requiring agencies to remove silos and adopt integrated strategies for holistic assessment and management.

The 2026 Mandate for Audit Committees*

1. Understand technology's impact on the control environment.
2. Reevaluate management's governance structure.
3. Keep pace with cybersecurity and data privacy risks.
4. Ensure balance between AI governance and AI investment.
5. Assess organisational talent and capabilities to innovate and address uncertainty.
6. Assess culture as a mechanism to drive ethical behaviour.
7. Understand and support internal audit's reinvention for the future.

* Audit committees are encouraged to self-assess their performance periodically. As a companion piece for this mandate, we have made available illustrative self-assessment questions.

1. Understand technology's impact on the control environment.

Under the Data and Digital Government Strategy, Australian public sector entities are rapidly adopting automation, digital customer interfaces, data-driven tools and artificial intelligence (AI) to improve service delivery and meet rising expectations. The Digital Access Standard encourages consideration of the end user experience, seeking to consolidate access points for Australians as they engage with government services. A recent review[1] of government efficiency commissioned by the Victorian Government recommended accelerating these activities to facilitate digitisation and automation of repeatable transactions across customer services, regulatory functions, corporate services and enabling infrastructure.

These developments can materially affect the operation of established internal controls. There is a risk that control impacts could become secondary considerations during system changes or digital transformation. This extends beyond managing risks associated with AI itself. While new technologies can streamline processes and be used to strengthen some controls, they may also weaken existing ones or introduce new risks, particularly where processes are redesigned or manual steps are removed. Modernisation efforts aimed at addressing technical debt can also affect controls in the short term, although system modernisation can generally be positive for the control environment.

Audit committees should ensure that chief information officers (CIOs), chief financial officers (CFOs), internal auditors and other senior executives actively advocate for maintaining a strong control environment throughout the planning and implementation of technology initiatives. Many departments and agencies operate within complex technology environments made up of multiple enterprise resource planning (ERP), human resource information (HRIS) and customer relationship management (CRM) systems, bespoke legacy platforms and operational technology. Dependence on third parties and evolving cybersecurity risks linked to technology deployments further intensify the need for strong oversight. The bottom line is that technology change can have a significant impact on key internal controls.

[1] Independent Review of the Victorian Public Service

Why it matters

As public sector agencies accelerate adoption of AI, automation and modern platforms, the design and effectiveness of internal controls will increasingly determine whether these changes strengthen or destabilise operations. Technology can improve efficiency, but overlooking control impacts during transformation increases the likelihood of operational errors, cyber threats exposure and compliance gaps. Audit committees that insist on accountability, strong governance, alignment with strategies and standards, and proactive oversight can help ensure technology investments enhance resilience and customer experience rather than erode them.

Key questions to ask

- How are emerging technologies, such as automation, AI and cloud platforms, changing the design and effectiveness of internal controls and are the right executives advocating for sustaining the control structure during implementation planning?
- Where might weaknesses exist in the control environment due to either reliance on outdated systems or insufficient planning for technology-related risks as these systems are updated?
- Is the audit committee receiving assurance regarding technology modernisation and AI initiatives to avoid blind spots in the control environment and to facilitate alignment with whole-of-government strategies?

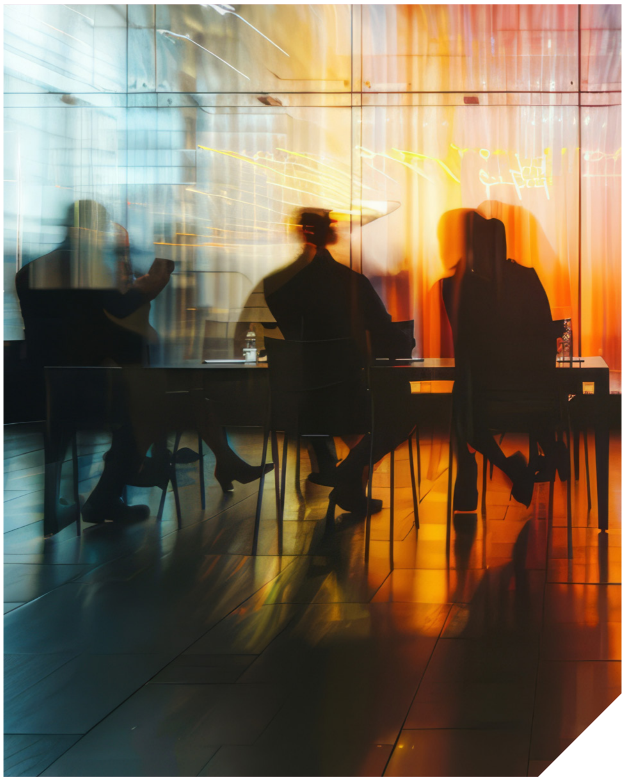
2. Reevaluate management's governance structure.

Audit committees in the Australian public sector play a critical role in advising the Secretary or Accountable Authority on whether governance structures are well designed and operating effectively. This advisory relationship (distinct from private sector audit committees that report to a board) creates a different dynamic, making visibility into how governance functions across the organisation essential.

A key element of this governance oversight is assessing whether the Three Lines Model spanning risk owners, risk oversight functions and internal audit is delivering the intended benefits of accountability, transparency and resilience in the rapidly evolving public sector environment. Although widely adopted, the model's implementation often faces challenges. Many departments and agencies struggle with defining boundaries, coordinating activities across divisions, or ensuring timely information flow. Issues may not be escalated promptly, while cultural resistance, inconsistent processes and competing operational priorities can limit collaboration and reduce the effectiveness of risk and assurance functions. These gaps heighten the risk of duplicated effort or unaddressed exposures.

Technology adoption in government agencies continues to mature. Entities are moving away from manual processes, yet the breadth of governance, risk and compliance (GRC) systems combined with legacy platforms, complex data environments and procurement considerations can add complexity. While centralising risk information supports consistency and improved visibility, partial implementations, or resistance to change, often delay expected benefits.

Audit committees should encourage management to periodically assess whether governance structures, systems, resourcing and cultural settings are enabling the Three Lines Model to operate effectively. Identifying where gaps exist will support meaningful improvements and strengthen the Secretary or Accountable Authority's ability to maintain robust governance in an increasingly complex environment.



Why it matters

As public sector entities navigate rapid regulatory, technological and policy change, strong governance helps maintain accountability and public trust. Without clear responsibility across the three lines or systems that support coordination, emerging risks may go undetected until they become significant issues. A well-functioning governance model empowers risk owners and internal audit, strengthening resilience, improving transparency and enabling more informed advice to the Secretary or Accountable Authority.

Key questions to ask

- Are roles and responsibilities across the three lines clearly defined, understood and operating in practice without duplication or oversight gaps, particularly in the context of statutory obligations and whole-of-government frameworks?
- Is there sufficient transparency, collaboration and timely communication between the three lines to support effective escalation of risks, alignment with strategic priorities, and compliance with legislative and regulatory requirements?
- Does the audit committee receive coordinated, consolidated and reliable reporting from each of the three lines to enable informed advice to the Secretary or Accountable Authority?

3. Keep pace with cybersecurity and data privacy risks.

As AI and other emerging technologies increase the scale and sophistication of cyber-attacks, audit committees must sharpen their oversight of cybersecurity and data privacy risks. Public sector agencies face escalating threats targeting government systems, high value datasets and critical infrastructure, while needing to meet compliance obligations under frameworks such as the Protective Security Policy Framework (PSPF), Essential Eight maturity requirements, the Security of Critical Infrastructure (SOCI) Act and the Privacy Act.[2]

Traditional governance models can struggle to keep pace with the rapid increase in the volume and variety of data that agencies are collecting, creating and storing. This includes the increasing volume and frequency of data sharing across departments and third parties, which creates an environment that is highly susceptible to exploitation.

For the second straight year, CFOs responding to Protiviti's Global Finance Trends Survey cited security and privacy of data as their top concern but many senior leaders are still overestimating their preparedness. A recent Harvard Business Review study[3] found that although 71% of executives believe cyber funding is adequate, only a minority view their governing bodies as proactive or innovative in managing cyber risk.

AI-enabled threats are worsening this challenge as cyber criminals are employing new techniques such as deepfakes, data poisoning, model inversion and automated prompt injection to conduct faster, more scalable and sophisticated attacks.

[2] *Navigating Australia's Cybersecurity Obligations: SOCI, PSPF and the Essential Eight — A Strategic Guide for Government and Critical Infrastructure Organisations*

[3] *Boards Need a More Active Approach to Cybersecurity*

Cyber criminals continue to target Australia due to the country's widespread adoption of digital infrastructure, perceived population wealth and varying levels of cyber maturity. The Australian Cyber Security Centre[4] noted increases in cyber security incidents and notifications issued to organisations in the 2025 financial year compared to 2024, which highlights the ongoing need for vigilance and action to mitigate against evolving and persistent threats.

Audit committees should actively engage chief information officers (CIOs), chief information security officers (CISOs), risk leaders and internal audit to gain a clear view of cybersecurity and privacy risks and to identify gaps where current investment or control assurance does not meet the organisation's risk tolerance. Audit committees should request more data driven reporting on how risks are being managed and how compliance with relevant policy and regulatory frameworks is being achieved to determine where internal audit coverage may not reflect the changing threat environment. This transparency will support stronger risk alignment and better-informed oversight across the organisation.

Why it matters

Cyber security and data privacy risks are central to the public sector's resilience and accountability, and its significance continues to grow with the adoption of AI, expansion of third party ecosystems and rising regulatory expectations. As threats continue to evolve, oversight must shift from compliance focused reviews to strategic assurance that tests how management anticipates, mitigates and communicates emerging vulnerabilities. An informed and engaged audit committee can reinforce accountability, drive appropriate investment and shape a culture of vigilance.

Key questions to ask

- What emerging cyber security and data privacy risks are affecting the organisation, and how is the audit committee obtaining assurance over management's mitigation activities, especially with the increase in the use of generative artificial intelligence?
- How is the entity evolving its cybersecurity and data governance strategy to meet future regulatory expectations, including PSPF controls, Essential Eight maturity uplift and SOCI Act obligations?
- Has the maturity of the organisation's third-party and supply-chain risk management program improved in line with increased reliance on external service providers?

[4] *Annual Cyber Threat Report 2024-2025*

4. Ensure balance between AI governance and AI investment.

Generative and agentic AI have the potential to reshape government service delivery models, increasing both the opportunity for innovation and the requirement for accountability, and calling for a greater need for assurance.

Under the Australian Public Sector (APS) AI Plan and with the help of GovAI, Australian public sector agencies are actively exploring and increasing the use of AI to improve efficiency and meet community expectations for service delivery. Meanwhile, internal audit functions across the public sector are beginning to experiment with AI to improve efficiency, analytics and coverage of assurance activities.

Many States and Territories are rolling out AI governance policy and guidance materials at varying rates and degrees of specificity. However, it is not yet mandated or common for State-based agencies to have established AI governance frameworks or clear accountability lines. Where there are gaps in policy ownership, model oversight, transparency and training, there is need for integrated governance rather than siloed technical adoption. Without clearly defined roles and handoffs and coordinated processes between technical, risk, legal, privacy and assurance functions, agencies may face what is characterised as "distributed responsibility without distributed accountability," which becomes a structural vulnerability as AI capabilities mature.

Audit committees should recognise management's dual mandates: investing in AI to raise agency capabilities while also ensuring that robust governance exists to manage AI related risks such as data integrity, privacy, ethics and algorithmic bias. Government entities tend to be appropriately risk averse and are often behind the private sector in emerging technology adoption. However, being overly cautious may result in missed opportunities to realise benefits. Setting up governance frameworks and clear accountability structures early can help fulfil the innovation mandate while being prepared for current and future regulatory expectations.

A practical approach to balancing AI adoption with risk management often begins with a cross functional AI governance council involving IT, legal, data privacy, risk, assurance and operational teams. Such groups help define strategy, roles, lifecycle controls and escalation paths. AI risk management should be embedded within the enterprise risk management framework and the Three Lines Model:

- **First line:** designing and operating AI related controls
- **Second line:** monitoring AI risks (e.g., ethics, bias, explainability, privacy, cyber)
- **Third line:** providing independent assurance and model oversight where required

Audit committees should oversee readiness for compliance with evolving AI and privacy regulations, the organisation's early stage use of AI in processes or internal audit, and the adequacy of internal controls supporting data governance and AI enabled decision-making.

Why it matters

AI is transforming how public sector entities deliver services and manage risk. Innovation is accelerating faster than traditional oversight mechanisms, making it essential for audit committees to ensure governance keeps pace with capability. When audit committees insist on clarity of ownership, sound control design and transparency around AI use, they help ensure emerging technologies improve service delivery without compromising integrity, compliance or public trust.

Key questions to ask

- How has the organisation defined ownership for AI governance, including roles across the Three Lines Model?
- Is the organisation balancing innovation and accountability, ensuring it is prepared to adopt AI responsibly as capabilities and regulatory expectations evolve?
- What frameworks or principles are being used to guide responsible AI deployment without stifling innovation?

5. Assess organisational talent and capabilities to innovate and address uncertainty.

Australian public sector organisations are operating in an environment of sustained fiscal pressure, rapid technological change and heightened public accountability. The APS Reform agenda and reviews, such as the Victorian Government's Silver Review, highlight a clear policy direction: future capability will rely less on traditional hierarchical structures and more on adaptable, digitally enabled and multidisciplinary skills.

The nature of public sector roles is changing. Automation and AI are reducing reliance on manual processing and transactional work, while increasing demand for skills in data analytics, digital service design, cyber security, AI governance, privacy and integrated risk management. At the same time, government policy settings are driving flatter structures and a stronger emphasis on delivery capability, collaboration and value for the money. As technology, data and automation increasingly shape public sector operations, agencies must ensure they have the talent and capabilities to manage new risks and realise emerging opportunities. Audit committees should understand whether the organisation is planning for these changes and whether its workforce strategy supports future service delivery expectations.

Public sector entities often face tight resourcing environments, capability shortages and competition for specialised skills. This makes it essential that agencies assess which capabilities must be built internally and where strategic use of external expertise, shared services or partnerships may be warranted. Audit committees should seek assurance that management has a realistic understanding of current workforce strengths and gaps, particularly in risk, information technology

cyber, assurance and data governance functions that are critical to maintaining control integrity during change.

Capability development should be integrated with broader organisational reform and digital investment programs. This includes ensuring that talent strategies address emerging regulatory and policy expectations, such as privacy, algorithmic transparency and responsible use of AI. Agencies should also prioritise learning and development to build adaptability, strengthen foundational governance skills, and support mobility across teams. Ensuring that workforce adjustments or automation initiatives are assessed for their impact on controls and organisational resilience is equally important.

By engaging proactively with senior leadership on these matters, audit committees can help ensure the organisation is building the capability base needed to manage uncertainty, respond to risks and deliver services effectively in a technology driven environment.

Why it matters

In a rapidly evolving environment, workforce capability is central to effective governance and service delivery. Technology-driven change, coupled with government-led workforce reform, means that having the "right people in the right roles" is no longer static, it requires continuous reassessment. Audit committees that understand current capability gaps and planned uplift are better positioned to challenge assumptions, anticipate risk and support sound decision making. A deliberate approach to capability development helps agencies remain resilient, maintain robust controls and meet public expectations.

Key questions to ask

- Does the organisation have a forward-looking workforce and capability strategy aligned to future digital, data and governance needs?
- Has the organisation gone through an honest evaluation of current capabilities and determined where the strategic use of third parties can close gaps in subject-matter expertise?
- How has innovation, including AI application, been incorporated into the talent strategy and resource development program?
- How is the agency addressing critical capability gaps — particularly in cyber, data, digital delivery and oversight functions — and determining where external support is required?
- Have technology-driven role changes and workforce adjustments been assessed for their impact on internal controls, risk management and organisational resilience?

6. Assess culture as a mechanism to drive ethical behaviour

A strong ethical culture is fundamental to public trust and to the effective operation of government. The Australian National Audit Office (ANAO) Integrity Framework[5] highlights that integrity, accountability and transparency are core expectations of all public sector entities, and that culture is central to preventing misconduct and supporting ethical decision making. In the public sector context where officials exercise authority on behalf of the community and manage public resources, culture is not only an internal driver of behaviour but a key component of organisational legitimacy and public trust.

Audit committees should not rely on informal or occasional updates on culture. Instead, culture should be treated as a standing governance topic, supported by structured insights such as behavioural indicators, survey trends, incident patterns, and data on the use of integrity and reporting mechanisms. Remote and hybrid work arrangements further underscore the need for ongoing monitoring, including signals such as communication tone, workload pressures and reliance on informal norms that may influence rationalisation of poor conduct.

Culture is often a leading indicator of emerging risk. Shifts in tone, transparency, or decision making can reveal underlying pressures, gaps in oversight, or vulnerabilities in fraud control. Audit committees should confirm that management's fraud and integrity risk assessments reflect contemporary public sector risks such as increased economic pressures, complex procurement environments, or the use of new technologies. Controls, such as segregation of duties, system access and automated monitoring, should be adapted as risks evolve.

[10] *ANAO Integrity Framework 2024-25*

Oversight should also include the effectiveness of whistleblower channels, escalation protocols and integrity breach response processes and not rely on an absence of reported disclosures as an indicator of cultural health. Entities need well practised mechanisms to address ethical breaches or integrity crises quickly, transparently and in alignment with legislative requirements. Regular testing and assurance supported by internal audit can improve preparedness and reinforce an organisational culture grounded in integrity, stewardship and accountability.

Why it matters

Culture is both a protective control and an early warning signal. When audit committees treat culture as a measurable element of governance, they gain visibility into behaviours that may indicate emerging integrity risks. Proactive monitoring — combined with clear accountability for ethical conduct and escalation — helps agencies uphold public trust, strengthen resilience and maintain the integrity expected of Australian public service organisations.

Key questions to ask

- Is management's approach to monitoring organisational culture measurable (e.g., aligned to the ANAO Ethics Framework), sufficiently robust and data-driven to act as a leading indicator of risk?
- Are mechanisms in place to support timely and transparent responses to integrity breaches, including effective whistleblower processes and escalation pathways?
- Has the organisation assessed how cultural pressures or rationalisation trends may influence fraud and misconduct risks, and are controls adjusted accordingly?

7. Understand and support internal audit's reinvention for the future

Audit committees should understand the chief audit executive's (CAE's) vision for the future of the internal audit function by reviewing its strategic plan and confirming that internal audit is taking proactive steps to stay aligned with emerging risks and developments. Public sector internal audit functions often operate with constrained resources and may not be early adopters of new technologies, yet they continue to explore opportunities to enhance efficiency, leverage data and remain relevant as an assurance provider within their organisation. Frameworks such as The Institute of Internal Auditors' (IIA) Global Internal Audit Standards and the Next Generation Internal Audit principles can help guide discussions about how internal audit intends to:

- Align its work program with organisational priorities, risk appetite and statutory obligations
- Use technology and data in a way that is appropriate to its capability and risk context
- Maintain agility and respond quickly to emerging risks, including those created by digital transformation
- Strengthen coordination with risk, compliance and other assurance providers to improve overall coverage
- Demonstrate conformance with IIA standards and operate as a strategic adviser

Generative AI and automation are beginning to influence global internal audit practice. While many agencies are still in the early stages of adopting advanced tools, some are trialling automation for data analysis, summarisation or anomaly detection to expand coverage and reduce manual effort. More advanced AI, including agentic AI, may eventually reshape testing activities, risk sensing and continuous auditing. However, this will require new skill sets, strong governance and safeguards to ensure controls and accountability remain intact.

A human-in-the-loop approach remains essential. AI may support repeatable tasks and enhance analytical capability, but internal auditors provide the judgment, context and stakeholder understanding necessary for effective assurance. The future focus is not only on how AI streamlines audit work, but how it enhances professional scepticism, insight and assurance quality. Internal audit must also be prepared to assess the organisation's governance of AI and digital initiatives, ensuring that associated risks are well understood and appropriately managed.

Through active oversight and partnership, audit committees can help internal audit modernise carefully, uplift capability and remain a trusted, independent function that strengthens governance and transparency across the public sector.

Why it matters

The increasing use of technology in government operations places new expectations on internal audit. Its ability to blend technology enabled techniques with professional judgment, ethical reasoning and organisational insight will determine its effectiveness. Audit committees that support capability uplift and responsible innovation help ensure internal audit continues to provide credible, independent assurance that strengthens governance and maintains public trust.

Key questions to ask

- Which parts of the internal audit process are currently incorporating technology or AI, and how are these tools being applied in a controlled and appropriate way?
- Does internal audit's strategy include the skills, training and external expertise needed to balance innovation with the human judgment essential to effective assurance?
- How is internal audit coordinating with other assurance functions to deliver integrated coverage of emerging risks, including those linked to digital transformation and AI?

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling organisations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the *Fortune* 100 Best Companies to Work For® list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Contacts

Rich Turley
Managing Director and
Government Lead,
Protiviti Australia
rich.turley@protiviti.com

Elly Maddy
Director, Internal Audit,
Protiviti Australia
elly.maddy@protiviti.com

Will Hunt
Director, Internal Audit,
Protiviti Australia
william.hunt@protiviti.com

Acknowledgements

Justin Yau and Rawan Nimer contributed to this piece.

Face the Future with Confidence®

11,000+
Protiviti professionals*

90+
office locations worldwide

25+
countries

$2 BN
in revenue*

The Americas

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

Europe, Middle East & Africa

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA*
Durban
Johannesburg

Asia-Pacific

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

© 2026 Protiviti Inc. Protiviti is not licensed or registered as a public accounting firm and
does not issue opinions on financial statements or offer attestation services. 0326-AU-EN

protiviti®