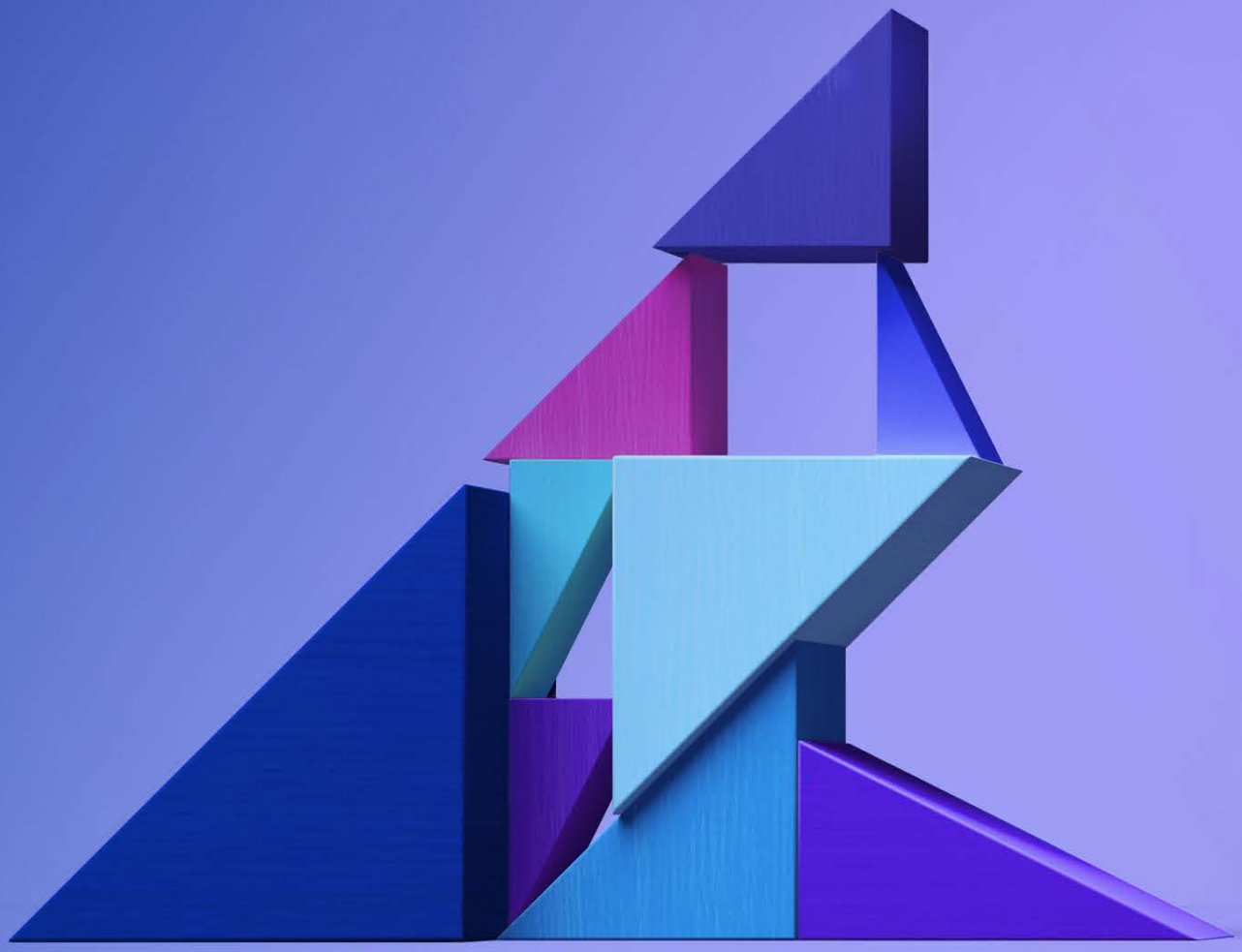
KPMG

Internal Audit in Focus FY24

An Internal Audit lens to the top risks organisations are facing



KPMG.com.au

To enable trust and add value, Internal Audit must remain agile and address contemporary risks. KPMG's Internal Audit team have worked through key focus areas for Internal Audit to consider in FY24.

Internal Audit in focus FY24

Macro-economics

The Australian economy has rebounded strongly over the past 18 months since the last lockdown period of negative growth in the September quarter 2021. Since then, Australia's unemployment rate remains low at 3.5% in February 2023. Wage pressure combined with general cost pressures has resulted in inflation increasing to its highest levels in nearly 40 years. The RBA has responded by raising the cash rate by 350bp since May 2022, to further slow demand and bring inflation back towards the target band. The short-term economic outlook is one of a significant slowdown in consumption and investment activity, with production slowing and profits squeezed.

From an organisational perspective, it is likely working capital pressures will increase as debtor days blow out and input costs rise. Organisations will need to balance these pressures in an environment of continued strain on global and domestic supply chains, requiring continued management of inventory levels.

Fraud and financial crime are likely to increase as individuals face personal financial pressures.

Internal Audit response

Internal Audit must be attuned to emerging risk and ensure the first and second line continue to evaluate external forces which may impact the organisation. Internal Audit should monitor risks from third party supplier exposures to economic shifts, whilst focusing internally on cost control, working capital management and understanding of debt arrangements.

Internal Auditors should, during every audit, identify potential fraud risks, evaluate the effectiveness of controls that prevent and recognise fraudulent behaviour, as well as conducting targeted data analytics to identify indicators of fraudulent conduct.

Geopolitical

The 2023 Edition of the World Economic Forum's (WEF) Global Risks Report coined a new word to describe the situation where a multitude of material problems and troubles occur simultaneously: a 'polycrisis'.

The pandemic remains a global threat (including effects of long Covid) as does the climate crisis and the ongoing conflict between Russia and Ukraine. Other emerging risks and issues that are more prominent include demographic shifts accelerating in China, supply chain disruption, monetary policy response to rising inflation and consequent cost of living impacts.

Energy markets and energy transition will continue to be impacted, including through continued disruption to energy trading from the Ukraine war, resulting in government policies to limit rising energy prices, and country competition for the capture of value in the clean energy transition.

Internal Audit response

Internal Audit should identify and address potential weaknesses in relation to compliance with international sanctions, as well as assessing how key geopolitical factors may impact an organisation's operation, such as investment decisions, dealings with overseas clients or disruptions to supply chains such as energy, raw materials or technology components.

Internal Audit should support organisations to remain vigilant to geopolitical uncertainties and ensure that organisations understand and have assessed impacts from political, social and economic disruption through scenario analysis, modelling and understanding interdependencies between geopolitical risks and other risks.

Talent has strengthened its grip on the top spot, with 77 percent of leaders nominating it as their biggest challenge in 2023 compared to 69 percent in last year's survey.

KPMG'S KEEPING US UP AT NIGHT 2023

People and talent

Covid has accelerated remote and flexible working, whilst also impacting the free movement of workers, resulting in our highest levels of labour force participation. Whilst uncertainty exists around potential macro-economic impacts associated with a slowdown in consumption and investment activity, including freezes on recruitment and headcount reduction, talent remains a key issue for organisations.

Organisations are grappling with a number of shorter-term people and talent challenges, including:

- **Culture** – the new hybrid model of the workplace and keeping workforces connected, engaged and working to a common purpose.
- **Learning** – the nature of learning and development in a virtual world and the need to adjust traditional learning methods.
- **Return to the office** – balancing the flexibility provided through working from home and the return to the office.
- **Technology** – exposures due to remote working (refer cyber) and upskilling of the workforce to meet a more digitised future.
- **Retention of talent** – remuneration increases have been challenged to keep pace with cost of living increases, increasing risk with regard to retention of existing talent and management of remuneration budgets.
- **Talent acquisition** – unemployment remains low resulting in a continued skills and talent shortage. Organisations are faced with a smaller pool of talent who increasingly demand flexible work, attractive remuneration and personal alignment with the organisation's purpose and social responsibility agenda.
- **Wellbeing and psychosocial obligations** – the impacts of the pandemic on wellbeing and new legislation focused on the management of psychosocial hazards in the workplace. Psychosocial hazards may be event-based (bullying, violence), or could be cumulative (job demands, poor support, low recognition, etc.).

Internal Audit response

Internal Audit has a key role to play in assessing people and talent risks, including:

- strategic workforce planning activities aligned to the organisation's future strategy and workforce needs
- talent attraction, talent retention and succession planning programs
- understanding the impact of employee departures, role vacancies and recruitment freezes on the internal control environment
- readiness for and assessment of psychosocial risks.

Organisational trust

An organisation's trustworthiness and the culture of trust that underpins it are fundamental to its success. Gaining and maintaining the trust of key stakeholders such as employees, customers, investors and regulators is critical, but this is no longer enough. The voices of those in your supply chain or the community in which you operate are also key. It is critical that organisations understand and respond to the sentiment of direct and indirect stakeholder groups.

In recent years, there has been a shift in the mindset of prospective recruits and employees when selecting their employers of choice. No longer is remuneration the key driver of where people choose to work. Rather, factors such as flexibility, workplace culture and the ability to do purposeful work for organisations with strong social values are more prevalent.

Similarly, customers are increasingly making conscious choices about the integrity and credibility of the goods and services they are buying, together with the buying experience. Regulators and investors are seeking evidence of organisational trustworthiness through transparency, integrity and accountability for compliance and related disclosures.

Organisations that fail to articulate and embed a compelling employee value proposition, who are not aware of the preferences of consumers, or who fail to meet compliance and performance expectations, will find themselves battling to retain talent, and maintain brand integrity and market relevance.

Internal Audit response

Internal Audit should consider how governance structures, systems and processes provide accountability and monitoring over the factors that impact organisational trust or published commitments. For example, this may include values or commitments related to taxation and remuneration transparency; local, indigenous and apprentice recruitment; modern slavery and ethical sourcing within the supply chain; progress in achieving ESG targets; or appropriate data collection and storage.

Internal Auditors as part of every audit should question how each process contributes to and exemplifies the organisation's purpose and values.

Privacy and data

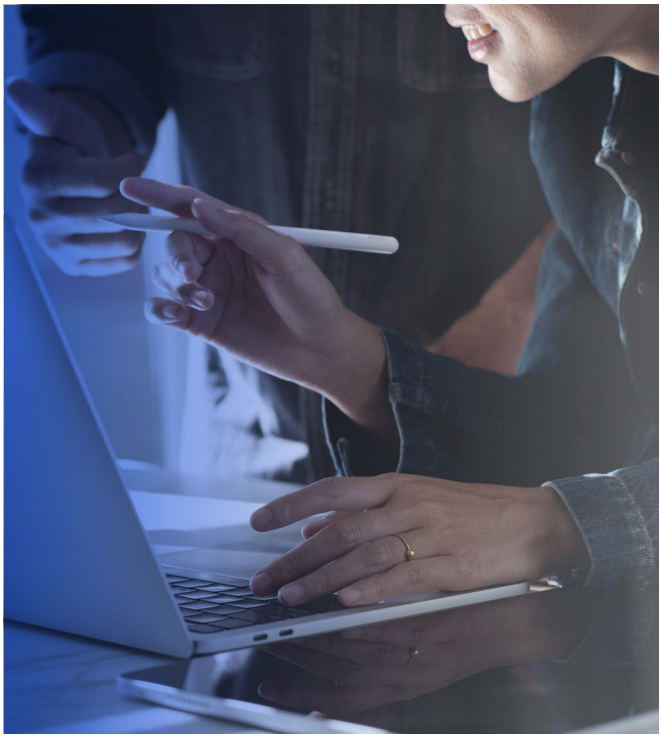
While technology advancements continue to be central to organisations' growth and efficiency agenda, customers, employees and regulators are increasingly concerned about the protection and use of their personal information.

2022 saw high-profile, significant data breaches resulting in widespread community impacts and increased awareness of vulnerabilities to malicious attacks. Organisations face increased financial penalties for serious or repeated privacy breaches, as well as reputational ramifications, if privacy, security and data practices are not effective.

Organisations must determine, both legally and ethically, what data to collect, what data to retain and for how long, what controls protect it, and what and how are decisions made based on it.

Internal Audit response

Internal Audit should assess privacy and data protection controls related to how, why, and what data is collected, stored, secured, retained and disposed of, in line with regulatory and societal expectations. With the rise in algorithmic prediction and AI, Internal Audit must also ask questions regarding how and why the information is being used. Internal Audit should also understand what third party providers have access to or host an organisation's data and the controls which protect its use.



Resilience

The current economic, geopolitical and environmental landscape facing organisations highlights the importance of robust and resilient systems, and the critical workforce which supports it. Events such as the pandemic and Ukraine conflict demonstrate the interconnectedness of risks and the concentration of risk when events occur. Preparedness for disruption is critical to not only survive disruption but thrive through it.

For example, the effects of and planning for climate change is placing pressure on organisations to adapt and thrive. The strength and frequency of extreme weather events, as seen through significant flooding throughout the eastern seaboard in 2022 and northern Western Australia in early 2023, generated significant pressures on organisations' systems, creating supply chain disruption and damaging vital infrastructure. Organisations must ensure their operations have planned for and are resilient to these changing weather impacts.

Similarly, the pandemic placed pressure on the resilience, flexibility and skills of workforces to maintain operations safely. Organisations must understand the composition of their critical workforce, what roles and depth of resourcing is required, what skills are required now and to meet future organisational needs (e.g. digital operators, contemporary energy skills), and what options exist through automation or leveraging of contractor arrangements.

Internal Audit response

Internal Audit must be attuned to external forces which may impact the organisation, and understand if an unforeseen event were to occur, how the event would manifest itself. In assessing threats to resilience, it is important that Internal Audit understand what matters most to customers and key stakeholders and bring these various viewpoints together – such as supply chain, cyber security, technology, third party risk, facility management, health and safety, regulatory and business continuity specialists – to ensure all aspects, strategies and resultant impacts are considered. Internal Audit must ensure the organisation understands the impact of potential disruption, what disruption would be intolerable, and the associated cost/benefit of resilience measures.

Regulation

The complexity and pace of regulatory change continues as technology, disruption, ESG and protection of individuals (privacy, consumer finances, psychosocial safety) drive regulatory bodies to respond quickly with new compliance requirements. Regulatory reforms (both proposed and enacted) reflect increasing efforts to enhance organisational resilience and respond to emerging technologies which don't fit within current regulations.

In addition to adapting to regulatory change, organisations must proactively develop – and more importantly maintain – a standard, agile approach to compliance which considers emerging technologies and is scaled across jurisdictions as both their footprint and regulatory expectations grow. Similarly, leading organisations are investing in automation to transform their operations, processes and even business models to drive resilience and agility to regulatory change.

Future regulatory approaches will likely transition from compliance with detailed rulebooks, to an outcomes-based approach focusing on whether the activities are safe and generate benefits for the customer.

Internal Audit response

Organisations need to continuously evolve their compliance efforts to ensure the control environment remains firm in the face of changing regulatory expectations and requirements, risk trends and emerging risks. Evolution in compliance is a necessity even when an organisation's risk profile has remained virtually unchanged.

Internal Audit should ensure the compliance operating model and management systems effectively meets the organisation's compliance obligations, mitigates risks of non-compliance, and can predict and respond quickly to changing regulatory and stakeholder expectations. Internal Audit should support management in identifying opportunities to enhance control activities through automation.

Cyber security

Cyber risks remain a top focus area for organisations. The business landscape in which cyber risk exists is fuelled by an ever-growing volume of sensitive data moving across interconnected and integrated networks. Recent high-profile cyber incidents have spotlighted the need for secure and resilient systems to protect this sensitive data.

The Australian Cyber Security Centre (ACSC) notes in their 2021–2022 Annual Cyber Threat Report that Australians report a new cyber incident every seven minutes; presenting cyber risks that can result in serious regulatory breaches, financial impacts, and loss of consumer trust. Organisations must understand what these risks are and take action to mitigate them. The most prevalent threats being phishing, social engineering and ransomware, leaving data and systems vulnerable.

Internal Audit response

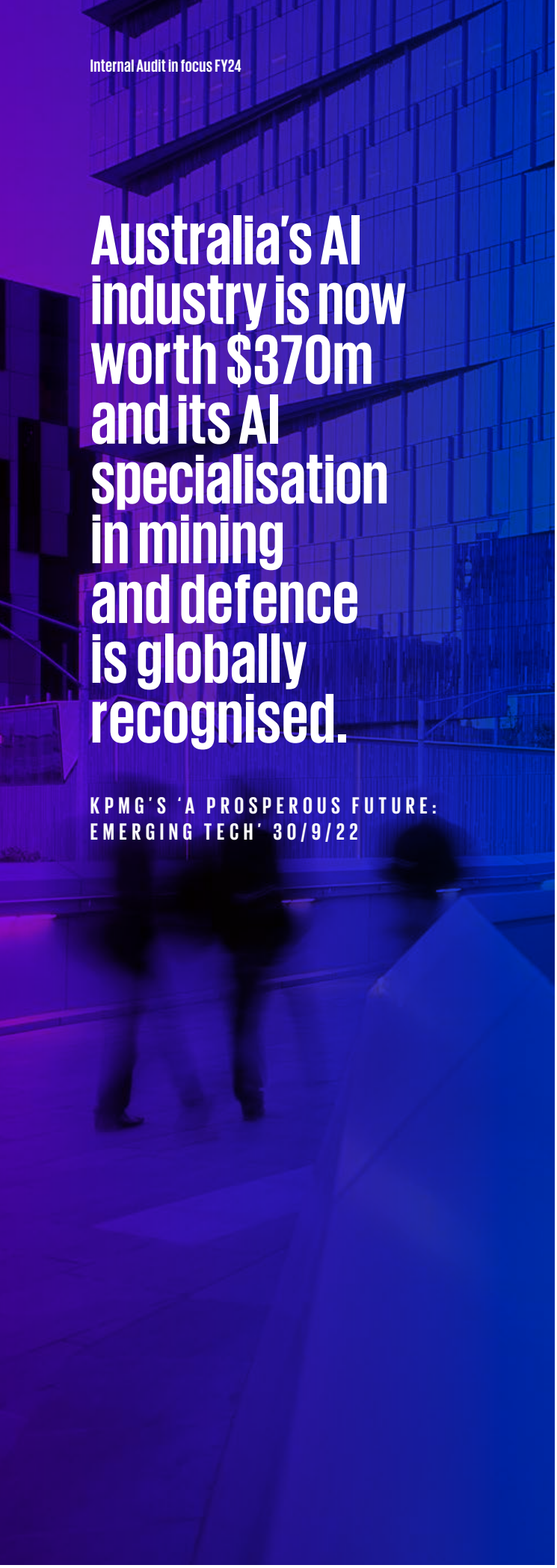
Internal Audit must continue to assess the veracity of controls to mitigate cyber security risks. Internal Audit must ensure the first and second line evaluate and communicate the effectiveness of cyber security controls on a continuous basis. Additionally, Internal Audit must move beyond traditional framework assessments to assessments of personal behaviours which impact on the organisation's ability to protect itself from cyber attacks.

KPMG's Australian Cyber Security Insights Report highlights

48% were less confident in their organisation's ability to subjectively assess cyber risks.

80% felt that AI/ML adoption raises unique cybersecurity challenges that must be prioritised.

75% believe collaborating with extended stakeholders, such as suppliers and customers, is vital to ensuring an organisation's cyber security.



Digital disruption

Many organisations are grappling with the risks and opportunities of digital disruption in one way or another.

Technological advancements, such as artificial intelligence (AI), blockchain, cloud computing, and the Internet of Things (IoT), continue to drive digitisation. In customer service, the use of chatbots is providing instant and personalised support to customers through messaging platforms, websites, and mobile apps. The rapid growth of generative AI applications, such as ChatGPT, represent significant business application through the automation of human tasks and processing of complex data. In supply chains, machine learning has transformed the way demand forecasting activities are completed, identifying patterns to predict future demand.

Changing societal attitudes have driven and demanded digitisation. In the workplace, many people have shifted to remote work and virtual interactions. At home, people are using digital devices to conduct everyday tasks including ordering food and interacting with healthcare providers. Organisations have similarly pivoted to new business models through e-commerce, contactless payments and buy now pay later implementation.

Continued focus should remain on data protection, privacy and the ethical use of these emerging technologies within the organisation and increasingly through the extended enterprise of suppliers and business partners.

Internal Audit response

As organisations embrace emerging technologies and new ways of business, the Internal Audit plan must remain agile and adapt to changing business processes. Internal Audit must ensure the risks and ethics associated with these changes have been assessed and appropriate controls and governance implemented.

Internal Auditors need to continuously upskill their technical knowledge to keep pace with the latest trends in technology.

ESG

More countries are moving toward global best practice and society are demanding higher-quality disclosures with evidence of progress towards ESG goals. Mandatory ESG requirements will come into play, as the International Sustainability Standards Board (ISSB) finalise their comprehensive global baseline of Sustainability and Climate Disclosure Standards.

This momentum will require the development of comparable metrics, access to quality data and data management strategies to assist monitoring and measuring ESG delivery promise and performance. COP27 has placed a significant emphasis on prioritising a shift to a decarbonised economy with energy transition at its heart. Organisations must understand the transition risks to achieving their ESG objectives.

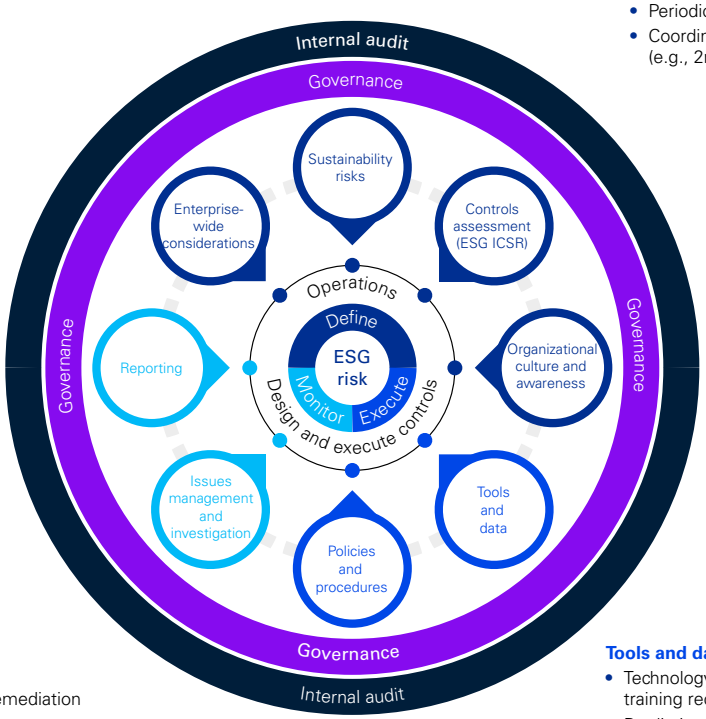
Internal Audit response

Combining the shift toward mandatory reporting requirements and the amount of capital committed to ESG transition, Internal Audit has a key role in supporting organisations to effectively manage ESG risk.

Enterprise-wide considerations
- Definition of ESG
- Mission, vision, values and strategy
- Periodic review by top management
- Context and stakeholder analysis
- Time, resource and budget

Sustainability risks
- Risk (and opportunity) assessment
- Regulatory requirements
- New product review
- Third-party due diligence

Controls assessment
- Monitoring and tracking of regulatory change
- Process and control testing
- Periodic ESG risk program evaluation
- Coordination with other assurance providers (e.g., 2nd line)



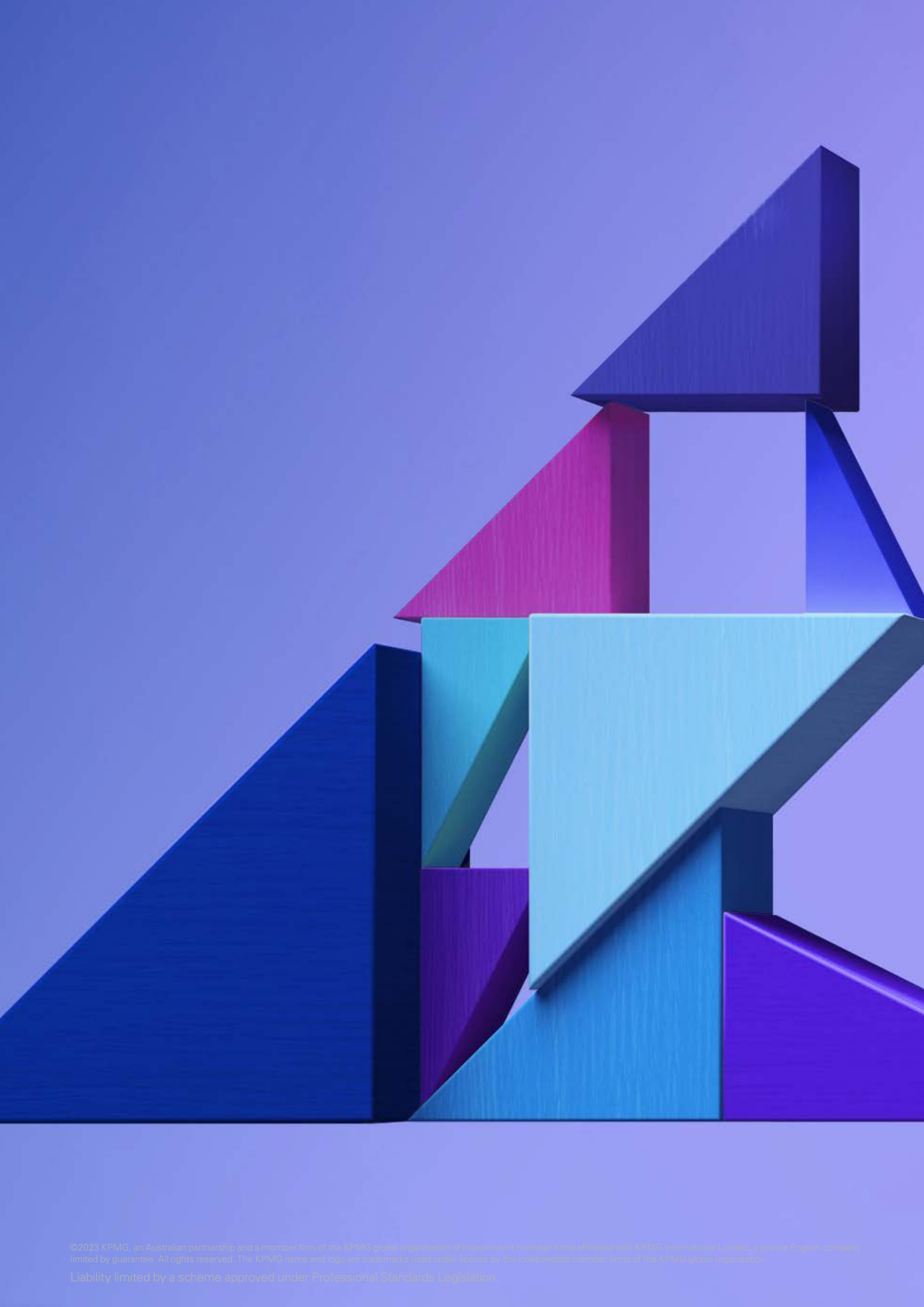
Reporting
- Probable regulatory reporting
- Periodic reporting to management and the board
- External reporting to stakeholders
- Record keeping

Organizational culture and awareness
- Engage and create dialogue with all the stakeholders
- Culture/tone of ESG/sustainability and behavioral change
- Regular and frequent training and communication

Issues management and investigation
- Issues/complaints management and remediation
- Responding to regulatory examination/inspection.
- Response plan and process for investigating alleged noncompliance
- Continuous improvement

Policies and procedures
- ESG policy existence and management
- Entity-wide policies and procedures (human capital, health and safety, cyber, lending and credit practices, investments, etc.).
- Consistency between policy frameworkand strategy

Tools and data
- Technology to support ESG program (testing, training records, etc.)
- Predictive measures: key risk indicators and key performance indicators
- Root cause analysis and trending
- Data governance/management



Contact us

Rowena Craze
National Leader, Governance, Risk & Controls Advisory
KPMG Australia
T: +61 7 3233 9682
E: rowenacraze@kpmg.com.au

Ben Lubach
Director, Governance, Risk & Controls Advisory
KPMG Australia
T: +61 7 3233 3182
E: blubach@kpmg.com.au

KPMG.com.au

March 2023. 1021878732AARC.