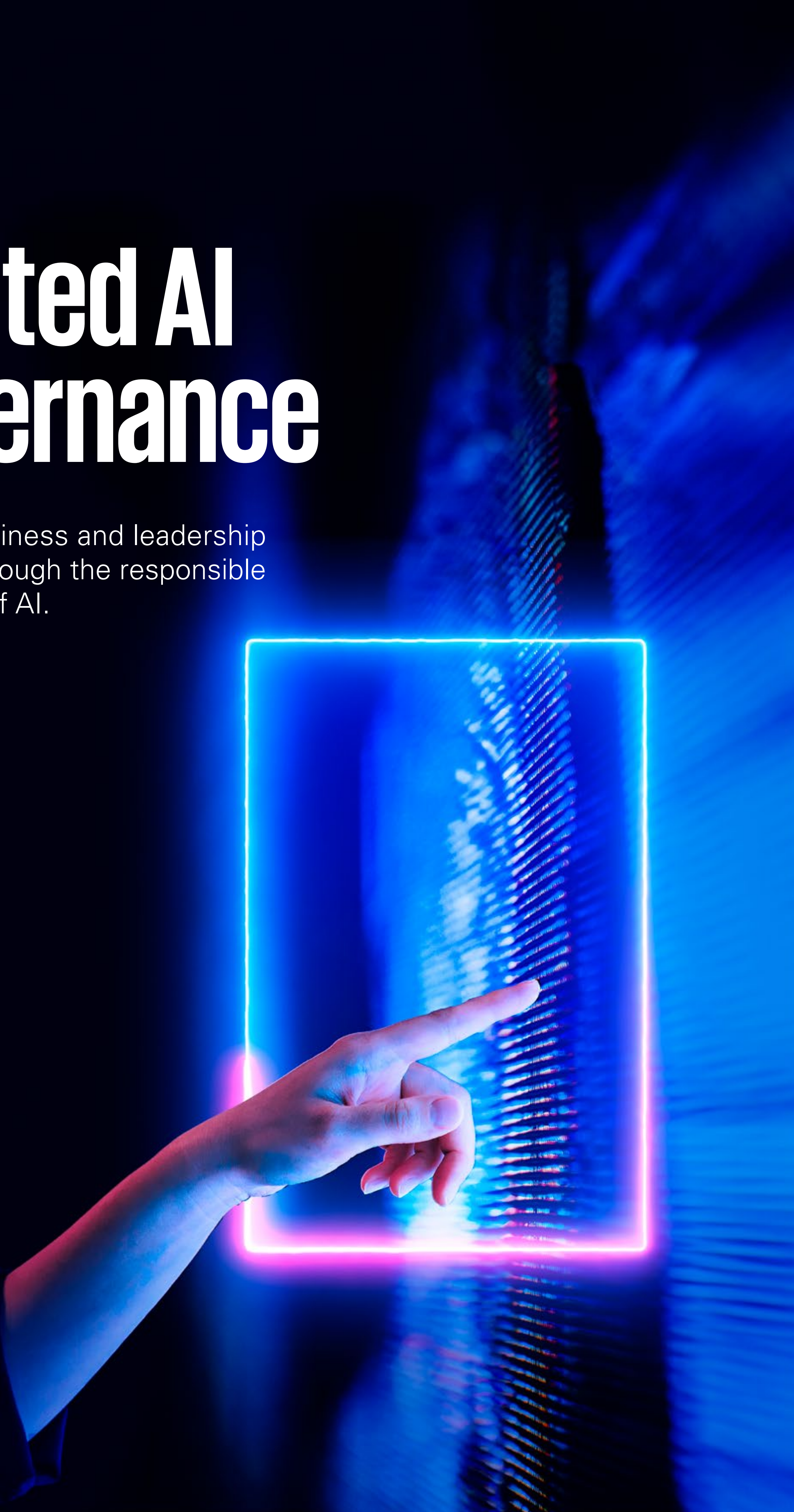
Trusted AI governance

Elevating business and leadership outcomes through the responsible governance of AI.



KPMG.com.au

As artificial intelligence (AI) promises to reshape the business landscape, organisations have to grapple with how to move fast, responsibly.

Rapidly evolving AI requires organisations to continuously adapt and learn, as they find new opportunities to reshape industries and drive economic growth. Nearly 98% of CEOs say AI will provide value to their business.[1]

A recent CSIRO report shows that 68% of businesses in Australia have already implemented AI technologies, and a further 23% are planning to do so in the next 12 months.[2]

While AI offers opportunities to enhance efficiencies and create value, it also introduces multiple risks which, if not identified and managed, can damage an organisation and cause harm to people and the planet.

[1] Workday, C-Suite Global AI Indicator Report, June 2023

[2] Hajkowicz et al, Australia's artificial intelligence ecosystem: Catalysing an AI industry, March 2023, CSIRO

Challenges exist, including around ethics, data privacy, security and the displacement of human roles. Businesses that successfully navigate these challenges can gain a significant competitive advantage.

How to most effectively use and address the ethics of artificial intelligence (AI), machine learning (ML) and other new technologies is the sixth greatest challenge keeping Australian business leaders up at night, and rises to second place when those business leaders look ahead to the challenges of the next three to five years.[3]

KPMG's 10th annual CEO Outlook, which surveyed 1,325 CEOs across 11 top economies including Australia, offers insights into the strategic direction and concerns of today's CEOs. This year's survey reveals that Australia's business leaders are betting big on AI, focused on bolstering their workforce and taking responsible steps forward to finding sustainable growth[4].

58% of CEOs say Gen AI is a top investment priority, despite an uncertain economic environment.

75% of CEOs believe C-Suite leadership has a clear idea on how Gen AI would benefit their companies.

42% of Australian CEOs think they have their data ready to safely and effectively integrate to Gen AI.

76% of CEOs did not believe Gen AI would impact on staff levels in their businesses.

If artificial intelligence (AI) solutions are deployed without the integration of critical controls and proper oversight and accountability, organisations may face regulatory, legal, reputational, and financial risks.

[3] KPMG Australia, Keeping us up at night, 2024

[4] KPMG CEO Outlook 2024, | Australia

The evolving regulatory landscape

The AI regulatory space is currently highly dynamic. Existing laws on consumer protection, corporate responsibility, cyber security, discrimination and more apply. Some laws, such as Australia's *Privacy Act 1998* (Privacy Act), are in the process of being updated to take into account the unique risks associated with AI that are not adequately addressed by the legislation, and in some instances, AI-specific legislation has been adopted or proposed. The need for comprehensive regulation becomes more pronounced as AI systems become increasingly integrated into society. Crafting a regulatory approach to AI that encourages innovation while also mitigating risk is key to accelerating its responsible development and use.

Europe has led the way in AI-specific legislation, adopting a risk-based regulatory framework – the European Union's *Artificial Intelligence Act* (EU AI Act) – which came into force in August 2024. The Australian Government has also committed to pursuing a risk-based approach, starting with the release of the Voluntary AI Safety Standard, alongside consultation for developing mandatory guardrails for use and development of AI in high-risk settings. These proposed guardrails focus on organisational accountability for AI safety risks, transparency requirements and testing through the AI lifecycle and supply chain.[5] This will help organisations responsibly design, develop and implement AI solutions.

Complementing this evolving regulatory landscape is an emerging portfolio of international standards, with the most recent ISO/IEC 42001:2023 focusing on an organisation's AI management system. This addresses accountability directly, requiring roles and responsibilities for AI to be defined and allocated, and a process to be put in place for reporting concerns about the organisation's role with respect to AI.

[5] Australian Government Department of Industry, Science and Resources, Safe and responsible AI in Australia consultation – Australian Government's interim response, 2024

Unique risks associated with artificial intelligence (AI)

Accountability mechanisms for AI should build on an organisation's existing policies, processes and structures, augmenting them in ways reflective of the unique risks associated with AI.

The table below highlights key unique risks posed by AI:

RISK	DESCRIPTION
ALGORITHMIC BIAS AND FAIRNESS	The risk of embedding systemic bias into automated decision-making systems is substantial. Fairness audits and bias-mitigation strategies can help avoid brand damage, stakeholder alienation and regulatory action.
ALGORITHMIC COMPLEXITY AND UNCERTAINTY	As AI systems, especially those based on ML, increase in sophistication, the algorithms driving them become more complex, leading to unpredictable or non-intuitive behaviour in edge cases. This complexity necessitates robust validation and testing regimes, to model how AI systems respond to unusual or unforeseen scenarios.
DATA PROVENANCE AND INTEGRITY	The provenance of training data is critical, as it impacts the model's performance and fairness. It is vital to have visibility over the entire data pipeline, from collection to processing, to ensure the integrity and representativeness of datasets. Overseeing data provenance is akin to supply chain management for physical goods and is subject to similar risks and quality control measures.
DATA SECURITY AND PERSONAL PRIVACY	AI systems are often data-hungry, potentially exposing sensitive information to privacy breaches. Protecting this data is not only a technical challenge, but also a compliance and reputational one, as privacy breaches can lead to serious legal repercussions and loss of public trust.
EXPLAINABILITY	AI solutions have complex decision-making processes, making their outputs often difficult to explain. For stakeholders to trust AI-driven decisions, they must understand how those decisions are made. Explainable AI contributes to trust and is a strategic imperative, ensuring intervention in the AI-human loop when necessary.
HUMAN-AI COLLABORATION AND AUGMENTATION	By cultivating a workforce that sees AI as an augmentation tool rather than a replacement, there is an opportunity to leverage AI for enhanced decision-making, creativity and efficiency.
REGULATORY COMPLIANCE AND ANTICIPATION	The regulatory environment for AI is nascent, yet rapidly evolving. A proactive stance and advocacy for reasonable regulation can position an organisation advantageously. It is essential to anticipate the direction of regulation and integrate compliance efforts seamlessly with an AI strategy.
THIRD-PARTY RELIANCE	AI disclosure from third-party providers needs to be reliable, trustworthy and consistently risk monitoring. A third-party incident response program enables the organisation to rapidly identify, respond to, report on and mitigate the impact of incidents and failures.

To mitigate these risks, it is critical to establish a robust AI governance approach, embedding clear systems, processes and oversight mechanisms.

Key elements of Trusted AI governance

As boards and the C-suite make strategic AI investment choices aimed at building a competitive advantage, they must at the same time evolve their approach to AI governance in a way that meets the maturity and complexity of their AI strategy.

The following eight elements are key for effective AI governance:

1. Leadership and accountability

Effective AI governance demands active engagement from senior leadership to set the direction and articulate the values that will guide the organisation in its use of artificial intelligence (AI).

While the specific governance model and structure adopted by an organisation will depend on multiple factors, the table below highlights the core roles to be played by organisational leadership.

ROLE	CONSIDERATIONS
Board of directors	– Define and communicate the organisation's AI risk appetite. – Ensure alignment of AI use with business goals. – Facilitate discussions on the development of a responsible AI framework, with supporting key performance indicators to monitor its effectiveness. – Allocate oversight responsibilities, including potentially augmenting the role of existing governance structures, or establishing an AI council. – Define reporting requirements, including where AI is used in the organisation and the risk management process. – Serve as an ultimate escalation point for ethical concerns raised through the organisation.
C-suite	– Establish an AI strategy, vision and responsible AI principles. – Create an AI management system that connects with relevant policies and processes and is supported by an overarching governance framework. – Encourage cross-organisational collaboration among AI developers, data scientists, risk, legal, privacy, security and business teams. – Develop and enforce risk mitigation strategies, including regular audits and assessments. – Establish strong governance practices to ensure data quality, security and privacy. – Participate in industry forums, regulatory discussions and standard-setting bodies. – Instil and model a culture that values ethical behaviours, accountability and transparency in AI initiatives. – Oversee the operational integration of artificial intelligence (AI). – Facilitate change management to align with the organisation's strategic and ethical standards.
Management and functional team	– Implement an integrated approach to AI risk management engaging risk, procurement and legal functions. – Develop and deliver capability building across the organisation to meet both general and role-specific skills requirements.

2. Principles, policies and standards

It is critical to design and/or adapt, socialise and operationalise comprehensive policies, processes and guidelines around the design and use of AI technologies.

These should focus on:

- ethical and responsible use principles (including, but not limited to, transparency and explainability)
- the data lifecycle – collection, quality, security, use, disclosure and disposal (including personal and sensitive information)
- revisiting existing policies and standards to align with AI governance.

3. Risk management and processes

Risk management protocols are essential to ensuring AI technologies are used safely and responsibly. These protocols enable an organisation to undertake risk assessments such as:

- privacy impact assessments
- security risk assessments to identify potential hazards (including security vulnerabilities and compliance issues)
- vendor management (including procurement and legal)
- other risk assessments (including business continuity, conduct and legal)
- escalations and challenge processes.

Once these risks have been identified, mitigation strategies can be developed and implemented.

4. Data governance framework

A data governance framework plays a pivotal role in ensuring the quality, security and ethical use of data throughout the AI lifecycle. This will involve establishing clear policies and procedures for data collection, storage, processing and sharing, to enable compliance with relevant regulations.

5. Cross-functional collaboration

Cross-functional collaboration enables the integration of diverse expertise, so organisations can address the multifaceted challenges associated with artificial intelligence (AI). Through open communication and regular interdisciplinary meetings, cross-functional teams can identify and mitigate risks, while optimising the AI solution's performance and goal to protect the organisation's data. Additionally, it encourages shared ownership and accountability, drives innovation and ensures AI deployments are effective and responsible.

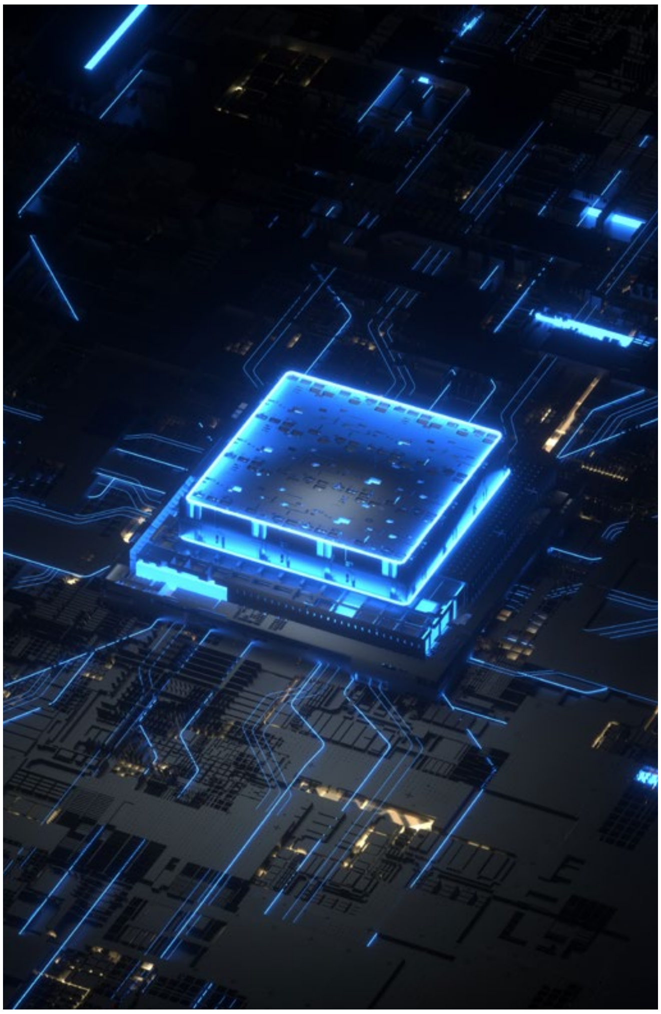
A key consideration is to engage an external independent expert in AI governance. This provides an additional layer of expertise and objective assessment and is now considered good practice in responsible AI management.

6. Supporting infrastructure

Supporting infrastructure encompasses the data sources and attributes, technology platforms and related systems required to support and implement governance practices.

This infrastructure often includes cyber security and data governance elements, to ensure all data ingested into an AI system is validated across data lineage, metadata and tagging, including:

- preparing the inventories of AI systems and data to identify their usage throughout the organisation
- implementing robust data governance practices across all systems, with a particular focus on those managed by third-party providers
- evaluating cyber security policies on AI systems to ensure their resilience and robustness, e.g. modernising and consolidating data platforms by decommissioning legacy systems can reduce the risk of data breaches and make data access more secure and efficient.



7. Culture, training and awareness

To embed artificial intelligence (AI) successfully into business operations, it is critical to foster a culture committed to ethics, transparency and continuous improvement. Organisational culture is an important part of defining an organisation's approach to risk and creates an environment conducive to sustainable innovation and the operational integration of AI.

Training and awareness of AI technology are also essential to equipping all internal stakeholders with the knowledge and skills needed to use AI effectively and ethically. Comprehensive training programs should be developed to cover various aspects of AI, including (but not limited to):

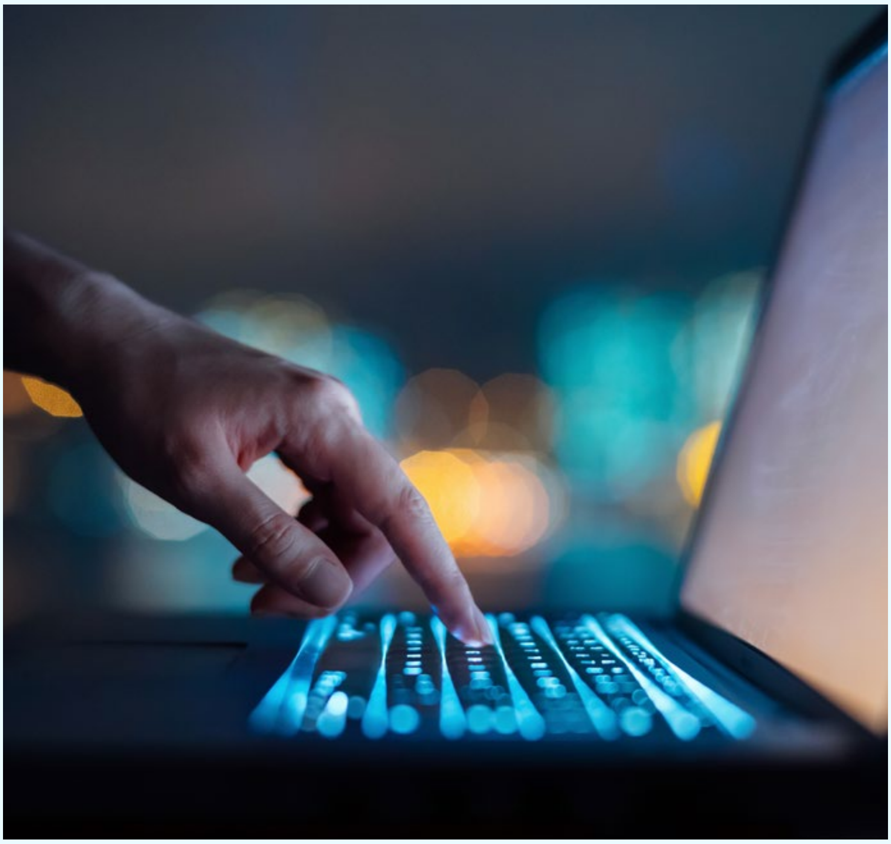
- technical skills
- ethical considerations
- data privacy and security
- regulatory compliance.

These programs should be tailored to different roles within an organisation, to ensure each group understands its responsibilities and the broader implications of AI use.

8. Continuous evaluation and improvements

Continuous evaluation demands a regular assessment of the effectiveness of the AI management system over time and implementation of a corresponding improvement plan. This involves:

- ongoing active engagement with all individuals and bodies with responsibility and accountability in the AI management system
- supporting continual embedding of responsible AI principles into the solution development lifecycle
- maintaining communications with and engagement of all relevant stakeholders
- continuous monitoring of the implementation of risk controls and performance of AI solutions against predefined metrics and responsible use standards – among other risks – biases, errors and security vulnerabilities
- ensuring alignment with evolving regulatory requirements, including regular external audits to enable an organisation to determine whether the artificial intelligence (AI) management system is compliant with regulatory requirements and industry best practice.



By making a commitment to continuous evaluation and improvement, organisations can maintain the integrity and efficacy of their AI systems, fostering trust and maximising long-term value.

KPMG offers a market-leading approach to the responsible and ethical design, development, procurement and use of AI, through our **Trusted AI Framework**.

The framework is based on three key principles:

1

Trustworthy

We can be trusted to uphold ethical standards and comply with applicable privacy and data protection regulations and confidentiality arrangements.

2

Values-led

We take a purpose-led approach that empowers positive change for our clients, our people and our communities.

3

Human-centric

We prioritise human impacts, as we embrace AI to empower and augment human capabilities.

Trusted AI governance: where to start?

Before defining an AI governance approach, has your organisation asked these fundamental questions?

Strategy alignment

- Is your organisation already using AI?
  - If yes, where and what controls currently exist to mitigate unique AI risks?
  - If no, have you assessed whether integrating AI into your organisation's business processes will address a strategic need?
- How can existing policies and processes, including in the areas of risk, procurement, data management, privacy and security, be uplifted to reflect AI-specific concerns?
- What new policies and processes are needed, e.g. AI policy?

Risk exposure and prioritisation

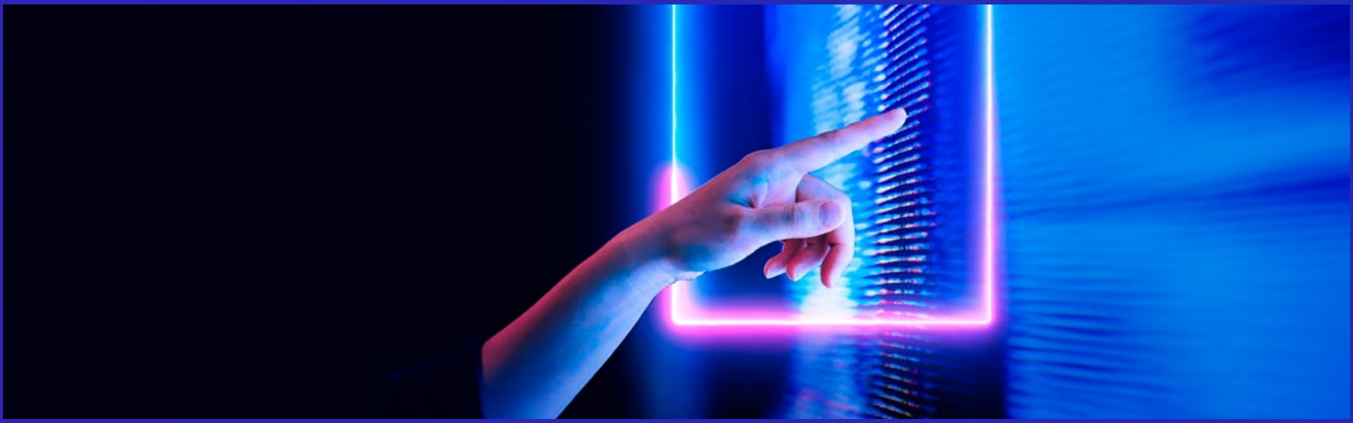
- What AI solutions are already in use by the organisation?
- What is the risk profile of the current or expected first-order use cases the organisation will pursue, particularly in light of the unique risks associated with AI and potential harm to people?
- What, if any, uplifts are required to the organisation's data management approach relative to the nature of the data to be used in the AI solutions?

Organisational structure, skills and training

- What existing governance structures could be leveraged in building an AI governance approach – or is a new body necessary?
- Would a federated or enterprise-level governance model be most appropriate for your organisation?
- Who are the key stakeholders that need to be engaged in the development and ongoing implementation of the AI governance process?
- What gaps need to be filled in the current skillsets of employees and leadership?
- What general and role-specific AI training needs to be developed and rolled out for all employees?

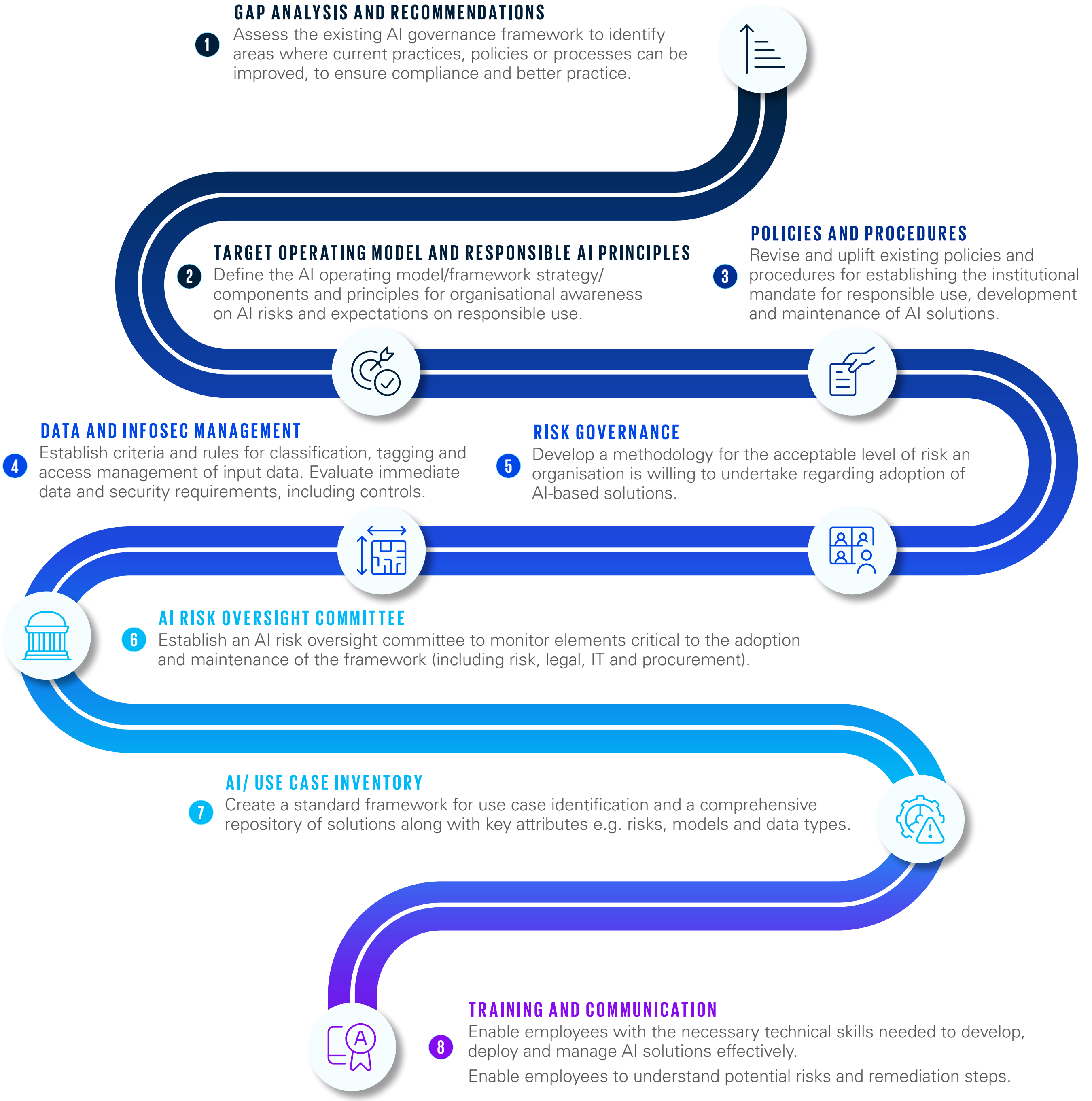
Tooling, continuous improvement and monitoring

- Has an escalation protocol been defined and documented for raising ethical concerns associated with the organisation's procurement, deployment and use of AI?
- On what cadence are technologies currently reviewed for performance and reliability, and in what circumstances should this be amended for AI solutions?
- Does your organisation have ongoing reporting and monitoring mechanisms in place?
- Has a periodic review process been defined to ensure policies and processes are current and up to date?



A roadmap to Trusted AI governance

KPMG has developed a holistic and bespoke approach to Trusted AI governance. We have a foundational layer of democratising responsible adoption of AI.



GAP ANALYSIS AND RECOMMENDATIONS

1 Assess the existing AI governance framework to identify areas where current practices, policies or processes can be improved, to ensure compliance and better practice.

TARGET OPERATING MODEL AND RESPONSIBLE AI PRINCIPLES

2 Define the AI operating model/framework strategy/ components and principles for organisational awareness on AI risks and expectations on responsible use.

POLICIES AND PROCEDURES

3 Revise and uplift existing policies and procedures for establishing the institutional mandate for responsible use, development and maintenance of AI solutions.

DATA AND INFOSEC MANAGEMENT

4 Establish criteria and rules for classification, tagging and access management of input data. Evaluate immediate data and security requirements, including controls.

RISK GOVERNANCE

5 Develop a methodology for the acceptable level of risk an organisation is willing to undertake regarding adoption of AI-based solutions.

AI RISK OVERSIGHT COMMITTEE

6 Establish an AI risk oversight committee to monitor elements critical to the adoption and maintenance of the framework (including risk, legal, IT and procurement).

AI/ USE CASE INVENTORY

7 Create a standard framework for use case identification and a comprehensive repository of solutions along with key attributes e.g. risks, models and data types.

TRAINING AND COMMUNICATION

8 Enable employees with the necessary technical skills needed to develop, deploy and manage AI solutions effectively.

Enable employees to understand potential risks and remediation steps.

Conclusion

AI is more than just a technology – it's a transformative force enabling unprecedented automation and decision-making, while redefining operations and the nature of competition.

Embracing artificial intelligence (AI) is a key driver for sustainable business success in today's rapidly changing digital economy, where organisations can use innovation to drive efficiency and value.

This power comes with a great degree of responsibility. Businesses are obliged to proactively design, operationalise and socialise AI governance, including developing clear roles and responsibilities supported by policies, processes, culture and controls, to build trust, promote transparency and ensure responsible AI development and use.

KPMG can help organisations to:

- build a responsible, human-centric AI strategy and governance structure
- assess current state maturity of responsible AI and future readiness, including in data, technology, competency and capability
- develop roadmaps to uplift human-centred AI maturity, informed by critical stakeholder engagement
- evaluate compliance against our Trusted AI Framework, the Australian Voluntary AI Safety Standard and other standards and regulation
- manage the spectrum of emerging and established risks associated with AI
- embed AI into operations for a competitive edge
- provide assurance over the organisation's AI governance framework, algorithms or specific solutions
- empower people to develop and use AI responsibly through learning, culture, and change initiatives that build confidence, engagement, and trust;
- build executive capability through workshops and providing support in setting executive accountabilities and reporting to the Board
- establish frameworks for the monitoring and evaluation of both AI solutions and people with reporting that drives a culture of continuous improvement
- accelerate the adoption and integration of AI technologies towards new ways of working, innovate, improve efficiency and provide better services.

This can help foster transparency and confidence in AI and serve as a foundation for innovation and new use cases.

Our interdisciplinary team draws on expertise across the divisions of KPMG Australia and globally, including law, privacy and data protection, regulations technology, human rights, governance, audit, assurance, risk and compliance. Our team also works directly with AI and ML practitioners and AI law and ethics scholars.

Contact us

Kelly Henney
Privacy & Data Protection Partner
Trusted AI Lead
E: khenney@kpmg.com.au

Warren Dunn
Partner, KPMG Risk
Consulting & Trusted
Solutions Leader
E: warrendunn@kpmg.com.au

Jessica Wyndham
Trusted AI
E: jwyndham@kpmg.com.au

Dr. Meg Brodie
Partner in Charge
ESG Social, Human-Centred AI
E: megbrodie@kpmg.com.au

KPMG.com.au

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

Liability limited by a scheme approved under Professional Standards Legislation.

October 2024. [1267937285C&M]