Developing your organisation's AI policy – *Key considerations*

In order to harness the opportunities of AI safely and responsibly, there is a need to establish a robust, holistic, and accessible AI policy that underpins the development, procurement, implementation and use of AI. Here are some key considerations that organisations should take into account when considering AI governance policies:

Key contacts

Adrian Chotar
Partner - Head of Digital, Cyber and Technology Law

T: +61 (0)457 808 068
E: *adrian.chotar@au.pwc.com*

James Patto
Director - Digital, Cyber and Technology Law

T: +61 (0)431 275 693
E: *james.patto@au.pwc.com*

Dealing with AI incidents and issues

Consider how issues with AI will be identified (i.e what is an issue from an AI perspective?) and reported by stakeholders, including employees and customers. Organisations will need to also consider whether workarounds exist where a system is under investigation/not available.

Consider establishing separate AI incident reporting mechanisms within the organisation to address issues with AI.

Criteria for assessment of AI systems

Businesses should consider what criteria or framework will apply to the assessment of AI systems. What criteria be applied in assessing whether AI systems present appropriate risk/reward balance to the business (i.e NIST AI RMF 1.0 - Trustworthiness).

Clear criteria should be developed in relation to the AI systems and use cases assessed by the organisation.

A clear definition of "AI"

AI is a nebulous concept. Organisations need to consider what AI is to provide clarity around when the policy does or does not apply. As a result, it is critical to ensure a functional definition of "AI" is established that sets clear boundaries for the policy.

When drafting, it is important to ensure that "AI" is defined to both emphasise technical functionality and facilitate clarity around policy implementation.

Other organisational policies

The AI policy should build on, and interoperate with, existing technology and data governance foundations – but organisations should identify any current policies requiring update such as privacy, IT security and third-party risk.

Organisations can leverage existing technology and data governance processes for AI systems. Existing third-party risk questionnaires and processes should also be revised to address AI.

Legal and regulatory requirements

Consider Australian and international regulation, principles and guidelines that have relevance e.g. Australia's AI Ethics Framework, NIST AI RMF, and other applicable laws (e.g. privacy, intellectual property, surveillance, human rights, business conduct rules etc.).

Consider undertaking a regulatory scan to determine applicable laws and how it might impact an organisation's use of AI prior to drafting a policy.

Approving AI systems and use cases

Thought should be given to how the organisation intends to use, develop or procure AI, which should be clearly stated in the policy. Organisations should ensure that any AI governance policy is paired with an appropriate process for approval of certain AI systems and use cases.

Consider an allow-list approach to AI, leveraging an organisation's existing technology governance structures to approve AI systems and uses.

Risk-based classification of AI

An AI policy should take a risk-based classification approach to AI systems and the proposed use cases based on the organisation's risk profile. The greater the risk posed, the more robust the controls and governance should be in place to address those risks.

Different AI use cases will require different levels of human involvement and risks. The higher the risk, the stricter and more defined the AI policy should be around required controls – including banning certain uses.

Ongoing assurance

AI is not set and forget. It is extremely important to set obligations around ongoing assurance, monitoring and testing of AI systems to ensure that they remain aligned with the organisation's requirements and obligations.

Organisations will need to consider what assurance related obligations they will place on AI system owners within the organization to ensure monitoring and ongoing compliance.

Holistic assessment and value alignment

Adoption of AI must occur with an ethical mindset, considering the holistic risk of harm to the organisation, people and society. Ultimately, the approach should be consistent with the organisation's values and the expectations of its stakeholders considering these wider harms.

It is important to ensure that the organisation approaches AI in a holistic manner and with the same ethical lens it approaches business and considers stakeholder expectations.

Transparency and accountability

Trust is a key enabler of digital transformation. The AI policy should clearly outline how AI is being used within the organisation to ensure key stakeholders are well-informed. It should also ensure clear lines of accountability for the use of AI in the organisation.

Identifying who within the business is accountable for particular AI systems and ensuring transparency in relation to how those AI systems operate is integral.

Governance operating model

Organisations should consider their AI governance structure at organisational level. Organisations can consider establishing an AI Board that supports a centralised governance and decision-making process for AI. This body should consider education of staff on the policy and guide how to apply it correctly.

An effective AI governance model should be based on existing technology governance structures, business' corporate values, ethical principles, and law.

Trusted AI

Accelerate responsibly.

pwc