SAP AUSTRALIA

SAP RESPONSE TO THE SAFE AND RESPONSIBLE AI DISCUSSION PAPER

SAP Australia

August 2023

SAP RESPONSE TO THE SAFE AND RESPONSIBLE AI DISCUSSION PAPER

SAP Australia Pty Ltd, a subsidiary of SAP SE (**referred to henceforth as 'SAP'**) a leading global software provider, would like to thank the Australian Government for the opportunity to contribute to the Safe and Responsible AI discussion paper (**the Paper**).

SAP is a major provider of corporate software solutions to critical industries and government across the Australian economy. For over 30 years we have continued to update these solutions to meet customer demand, evolving cybersecurity threats and Australian legal requirements.

SAP delivers Artificial Intelligence (**AI**) built for business. AI from SAP is built into the applications our customers use every day. It is relevant to their business because it is based on SAP's deep industry and process knowledge combined with business data and SAP's open ecosystem of general-purpose AI partners. SAP Business AI is designed with safety and responsibility.

At SAP, we believe that AI has great potential to create opportunities for businesses, governments, and societies. However, for people to trust AI solutions, the development, deployment, use, and sale of AI systems must be governed by clear moral rules.

SAP welcomes the discussion on the impact of AI technology on the Australian economy and its people. The investment and thought being applied by industry, academia, and government give us confidence that we are approaching this in the right way to ensure that the technology is used to improve the lives of Australian citizens and its economy. For this reason, we support a review of Australian regulations to manage the transformative impact of AI technology.

About SAP and its use of AI

SAP is a leading provider of business-to-business technology solutions and is excited about the opportunities that AI presents to improve the way businesses and governments operate. Our portfolio of solutions is used across the Australian economy, from mining and energy to consumer goods and government services.

AI technologies have been powering these solutions for over a decade. Given our critical role across economies, we recognise both the transformative nature of the technology and the potential harms that can arise from its unethical use.

SAP defines AI as the ability of a machine to achieve perform specific goals such as perceiving, reasoning, learning and problem-solving by using relevant data, algorithms and processing capacity. The AI requires a system to correctly interpret relevant data, learn from such data and use those learnings to achieve specific goals through flexible adaption.

We differentiate between two types of AI systems.

- **Rule based AI** – behaviour is fully defined by rules created by human experts. These systems are often described as symbolic or expert systems.

- **Learning based AI** – humans define the problem and the goal but the behaviour, rules and relationships required for the system are learned in an automised way. Using data they train how to solve a problem and continuously adapt their function to this process.

At SAP we operate against our Global AI Ethics policy to ensure that the development and deployment of SAP's AI systems are in line with established guiding principles and core organisational values. This policy is applied across the SAP's AI development lifecycle.

SAP's AI policy operates against three pillars

1. **Human Agency and Oversight** – allow human intervention for all automated decision processes
2. **Addressing Bias and Discrimination** – Ensure that AI methods do not result in inaccuracies detrimental to data subject rights.
3. **Transparency and Explainability** – Provide transparency when using AI during processing of personal data.

In addition to these pillars SAP prohibits the development of certain AI use cases.

Personal Freedom

- Human surveillance – where it is used for targeting individuals or groups with the purpose of disregarding or abusing the rights of individuals or groups.
- Discrimination – where it used to discriminate or exclude individuals or groups from access to AI benefits and opportunities to the wider population.
- Deanonymisation – where it issued to deanonmysie anonymised data to result in the identification of individuals or groups.

Society

- Manipulation – where it issued to deceive or unfairly manipulate individuals or groups via public forums, media or moderation of other similar uses.
- Undermine debate – where it is used to undermine human debate or democratic electoral systems.
- Intentional harm – where it is used to intentionally harm users and or those directly or indirectly affected by the system.

Environment

- Environmental harm – all systems shall be conducted with minimum to no explicit damage to the environment.

How SAP integrates AI technologies into our solutions

SAP provides AI that is built for business. SAP AI enriches business processes that are available in the systems that powers the most critical business functions. The AI scenarios are developed using extensive industry specific data and deep process knowledge and is created using responsible AI practices.

1. **Built into business processes**: SAP has built AI into the applications that power most critical business processes (such as Finance with AI). Business AI processes are available across Cloud ERP (S/4HANA), spend management, customer relationship management and human capital management. For example, SAP's intelligent intercompany reconciliation is an AI enabled process that helps retailers predict demand of when products will be sold, helping reduce inventories and waste across their stores. Another example is Concur, our expense management system, that uses Optical Character Recognition to read and digitise scanned receipts. It also intelligently organises receipts by work trip and supports organizations in recognising patterns of behaviour that may warrant further audit and checks.

2. **Relevant**: AI that is trained on industry insights, business process expertise and tailored to customer data. For example, using AI in supply chain management across SAP's Integrated Business Planning solution or retail specific replenishment applications.

3. **Infuse business specific AI into workflows:** SAP AI business services offers customers with the ability to extend certain workflows. There are low code/no code services available on SAP Business Technology Platform (BTP) that helps customers with specific automations. An example is using the AI document extraction service to read PDF documents and upload information to the transaction system.

4. **Deploy customer AI scenarios in SAP applications:** Our customers often store large amounts of business data on our platforms, be it financial, operational, or customer data. SAP offers AI tools built on our PAAS BTP technology platform that allow for analytics to be performed on that data to gain insights or improve the productivity of existing processes.

5. **Generative AI and SAP:** We use Generative AI in alignment with our overall SAP AI strategy, i.e., built for business and deeply embedded into our business applications and end to end processes. SAP combines the power of Generative AI with the context of business data and business processes. This process keeps humans in the loop responsibly to review and approve the generated information and the use of Generative AI follows the same ethical principles. For example, the rapid generation of job role descriptions in our HR platforms. An important principle on which this is designed is that business and customer data is not passed to the LLM to improve its algorithm. The data stays with the customer.

As a developer, SAP offers a toolset for businesses and governments to operate and interact with their customer base. While SAP partners with the best Foundation Models to integrate into our solutions, we do not operate LLMs. Our role in the supply chain is to enable our customers, rather than to use AI to generate business insights or operations.

While as a developer we do not have line of sight, or control of the application of these tools by our customers our AI solutions are designed to address specific business problems and as previously noted, in alignment with our Global AI Ethics policy we have prohibited AI Development use cases.

SAP views on the safe and responsible use of AI in Australia

SAP has the following key perspectives on the safe and responsible use of AI in Australia:

1. Regulation must account for the AI supply chain;
2. Interventions should leverage existing regulation;
3. Ensure a common set of principles for government AI and the application of regulation;
4. Regulatory intervention should take a risk-based approach;
5. A co-ordinating body and governance structure; and
6. The role of Government as an AI exemplar.

Regulation must account for the AI supply chain

Regulation should reflect the different roles and abilities of the organisations involved in creating and using AI. The responsibility and consequences of meeting those regulations should fall on the group best able to identify and reduce the risk of harm that made the regulation necessary. There should consequently be a distinction made between Developers and Deployers.

The two roles can be distinguished as follows:

- an organisation that designs, codes or produces an AI system, for example a system integrated into an expense management solution to read digital images of receipts is a **Developer**
- an organisation that uses that AI system to make a decision for a customer, employee or for its own business operations is a **Deployer**; and
- in some cases, the same organisation may be both a Developer and a Deployer.

A Deployer using an AI system does not generally have control over design decisions made and data used by the organisation that developed the system. Likewise, a Developer generally does not have control over the subsequent uses of the AI system by an organisation that deploys the system.

It is critical that Deployers have the necessary data governance practices in place to ensure the proper use of AI models provided by developers. Data used in AI applications is specific to the use case and Deployers should understand the associated risk of using poor quality or inaccurate data will have on the AI model's decision making.

AI regulation should make clear the responsibilities and obligations of AI Developers and Deployers. This ensures the appropriate organisation in the supply chain can identify and mitigate risk. Importantly from a citizen or customer perspective it ensures that lines of accountability are matched to the relationship between the end user and provider.

For example, transparency obligations as to the use of AI in high impact decision making would be best applied to the Deployer as they have a direct relationship with the customer whereas the Developer will have no relationship with the customer.

This distinction has parallels to the General Data Protection Regulation (**GDPR**), widely considered to be best practice privacy regulation which has the Processor / Controller distinction. The benefit of this distinction was recognised in the context of the *Privacy Act 1988* (Cth) ('Privacy Act') reforms which recommend amendments to the Act to incorporate the Processor Controller distinction.

Furthermore, a distinction can also be made between scenarios which involve direct interaction with consumers or citizens and business to business interactions. In the business-to-business context we would recommend a maximum freedom to contract to establish responsibilities and obligations on the entities best placed to comply with them and mitigate risks and understand the specific context and use-case.

Interventions should leverage existing regulation

There are a number of issues that have been raised with the increased prevalence and power of AI technology. For example:

- Generative AI creates believable images and videos of events that never occurred. This has the potential to create misinformation and unfairly damage the reputation of an individual, undermine democratic institutions, or infringe on the commercial copyright of an individual or business.
- The use of AI in autonomous vehicles is not always effective, and it could potentially result in harm to the driver or passengers. This raises concerns regarding consumer protection and product safety.
- AI-assisted decision making, which is built on incomplete or biased data sets, could result in unfair discrimination against an individual. The impact of such discrimination could be life-changing depending on the importance of the decision being made.

SAP recognises that governments will need to intervene to manage these potential harms. However, we consider that actions taken should build on existing regulation, rather than using a technology-specific regulatory approach. For example, considerations of the impact of AI on worker rights and employment conditions will be different to those on vehicle safety. Consideration on whether a government response is required will be best delivered by those policy makers and regulators responsible for those matters.

As noted by the Paper, AI is an enabling technology, as such it is often an element in other systems and technologies and used across industries. This will mean that AI is regulated under multiple laws increasing the likelihood of **duplication and conflict between** **regulatory systems**.

AI development often depends on the ingestion of large sets of data that are used to train algorithms to produce models that assist with decision-making. To the extent that any of the input for an AI model involves personal data, or any output is used to make decisions that affect the rights or interests of individuals, the AI model and its applications are already directly subject to the Privacy Act.

We support the existing approach taken by the Government where it has leveraged existing frameworks and avoid duplicating or creating any conflicting requirements with these frameworks while already promoting trust by enforcing existing legislation. For example, the Privacy Act, which already protects the use of citizen data in large data sets (an essential element for AI) and is considering measures to improve transparency on the use of Automated Decision Making.

To the extent it is not already being done, there is value in reviewing existing regulatory frameworks as they relate to consumer, data protection and privacy, corporate, criminal, online safety, administrative, copyright, and intellectual property laws against the potential harms from AI to determine whether they are fit for purpose. However, this should be done with an:

- understanding of the AI supply chain;
- application of a risk based methodology (see section *Regulatory intervention should take a risk based approach*);
- against set of common principles (see section *Ensure a common set of principles for government AI and the application of regulation*); and
- in a co-ordinated manner (see *A co-ordinating body and governance structure*)

Otherwise, there is a risk that over-prescriptive rules will hinder investments in AI as well as the use of innovative AI solutions.

Ensure a common set of principles for government AI and the application of regulation
The Australian Government should review the effects of AI against existing regulatory powers to determine whether action is necessary. Since this will require consideration from regulators and policy makers from various portfolios, the Government should establish a set of common principles to guide the assessment and ensure a consistent approach. These principles would guide policy making, reform and enforcement.

Globally and domestically, there are many existing AI ethical frameworks and principles that are applied by organisations utilising AI in the operation of their businesses. As noted previously SAP's Global AI Ethics Policy uses the principles of Human Agency, and Addressing bias, Discrimination and Transparency and Explainability.

A review of these global policies can be distilled to some common themes that are reflected in the UK Government's White Paper.

1. Transparency – How clear is it what systems and processes are AI enabled and to what extent can the basis for its decision making be understood?

2. Fairness/ Non-bias – To what extent does AI discriminate unfairly against individuals or groups?
3. Contestability – Within a decision-making construct enabled by AI to what extent can an individual challenge the decision or have it reviewed?
4. Safety – Does the AI system work robustly, securely, and safely?
5. Accountability – Is there sufficient oversight of decision making and are organisations accountable for the AI system to operate effectively and is there sufficient governance around decision making around the AI implementation.

Whichever principles the Australian government conclude on – what is critical is that these principles exist and form part of a mandatory framework for consideration of policy or regulatory intervention that impacts on AI technologies.

Regulatory intervention should take a risk based approach

The application of these principles to the AI related issue should be undertaken on a risk-based approach. Regulatory interventions should be scaled to meet the risk i.e. an assessment of the likelihood of harm against an individual or organisation combined with the severity of that outcome. For example:

- High Impact High Likelihood - The governance and assessment of an AI system used in an autonomous vehicle would more likely require some form of intervention or governance oversight
- Low Impact Low likelihood – An AI platform used by a business to optimise its inventory management system.

To reflect on the risk-based approach, it is essential to set up a clear and precise criterion for high-risk AI systems based on the probability of occurrence and consequences for individual rights and freedoms, security, or safety and how to mitigate such risks.

Any risk assessment should include assessing the benefits of a proposed AI application or the risks of not proceeding with the development or deployment of the AI application. This is just as important as focusing on the harm that may result from proceeding with the AI application and makes sure the use of an AI application is proportionate to the desired outcomes. There are many high risks with an AI system processing sensitive personal data (e.g. in healthcare) that would be outweighed by the benefits to individuals and society at large from such applications.

To conduct risk mitigation when using high-risk industrial AI applications, international standardisation bodies, driven by industry, should develop common standards for the use of AI in business. Policy makers should seek to advance innovation and promote a risk-based approach to AI that fosters trust, promotes harmonisation of standards, and support global alignment on AI through the OECD and other international for a and work with our allies to advance AI research and development.

The establishment of regulatory sandboxes are also essential for a risk-based approach. Here AI applications can be tested in protected legal environments to develop innovations and regulations with high practical applicability. In addition, joint experimental spaces for AI applications with partner jurisdictions should be pursued.

A co-ordinating body and governance structure

Given the cross sectoral impact of AI technology, co-ordination by government will be critical. This will require new ways of working and potentially cabinet endorsement of a formal approach that will require all government agencies to follow.

At the centre of this would be a government body to ensure no duplication of effort by organisations and individuals, no conflict between policy and legislative proposals, and where avoidance of overlap is not possible clear guidance on which rules should be followed by industry.

In acknowledgement of the independence of regulators – at a minimum the new body would be available to ensure all regulators remained cognisant of approaches being made by other regulators, alert them to potential areas of conflict and how other regulators were applying the principles.

This body could also be source of AI understanding and expertise that could support whole of government and regulator understanding of AI and emerging issues. This function should however be sub-ordinate to the key function which is to support co-ordination between policy makers and regulators.

Without co-ordination there is a risk of overlapping regulations that will hamper the ability of companies to develop AI-based innovative business models and thereby remain competitive at a global scale.

Regarding the creation of this body, we are agnostic as to whether a new statutory organisation is required or whether the function of the body could sit within an existing Agency. What is important is that the organisation is empowered to act as a central co-ordinating body across government.

The role of Government as an exemplar

We consider that there is also an opportunity for the Government to play a more active role in the use of AI in the Australian Economy. Governments play a critical role in the safe and responsible economy wide take up of AI as they:

- set and enforce data privacy laws;
- are responsible for large amounts of data;
- are large service providers;
- have IT budgets to deliver major projects; and
- are directly accountable to their citizenry.

Governments have an important role in influencing public attitudes to AI. If governments use AI ethically and responsibly, this will build public trust and acceptance of the use of AI across the economy. The Government must accelerate its use of AI in its systems of operation of government and service delivery.

This is also critical to good policy making. To make good policies about AI, you need to understand it well. This will only happen with greater use of AI within government. This will allow the government to best appreciate how it works, what the risks are and how to best mitigate them.

SAP's Institute of Digital Government has undertaken research into the use of AI within Government and its challenges. The research has indicated that there are four major challenges facing the government's use of AI.[1]

1. **AI is resource intensive** – To effectively utilise AI requires people with the skills to develop and use AI, the systems to undertake the analysis and the data sets on which to undertake the analysis – government agencies face challenges in all those matters.
2. **The right operating model** – Operationalising the use of AI requires new ways of operating – it requires a combination of data science skills along with policy domain expertise in the

[1] https://discover.sap.com/sap-institute-digital-gov/en-us/publications.html#:~:text=Leveraging%20Artificial%20Intelligence%20in%20Government

design and operation of the AI. This requires new ways of operating within typically separate areas within agencies

3. **Opaqueness of AI models -** Many advanced AI systems face the challenge of not being able to be understood by humans, the so called explainability problem This is a particularly a challenge for governments due to the potential ramifications of government decisions on an individual and the importance for governments to be able to demonstrate fairness and transparency in decision making.
4. **Cultural issues** – Perceived and actual impact on employment, challenges to established wisdom and concerns around the public's acceptance of AI within service delivery are all elements that impact on AI take up within the public sector.

AI is ultimately a tool, and its use should result in better business and government operations. If it fails to do so, its adoption within government will face challenges.

Currently, the adoption of AI technologies by businesses and governments is still in its early stages. Use cases are still being developed, and the application of the technology to existing processes is relatively new. This can understandably lead to reticence within government to undertake AI projects where the benefits are unclear or the capabilities are unproven. Like all new technologies, making a business case for their use when the results are unclear or unproven is challenging. Equally problematic is the high expectations on the insights the application of AI can provide, where there is a lack of clear understanding of what the AI can deliver.

However, all these challenges are surmountable, and the Australian Government, in partnership with industry, academia, and community organizations, must embrace AI technologies. We are seeing positive developments across the public sector to help with the growth of AI use. For example, the DATA Act will empower access to greater data sets across the economy. There is also a growing willingness by political leadership to ask how AI technologies can help make the public sector more efficient and deliver better customer services.

ATTACHMENT A

RESPONSES TO SPECIFIC QUESTIONS RAISED BY THE PAPER

Potential Gaps in approaches
What potential risks from AI are not covered by Australia's existing regulatory approaches? Do you have suggestions for possible regulatory action to mitigate these risks?
We support the existing approach taken by the Government where it has leveraged existing frameworks and avoid duplicating or creating any conflicting requirements with these frameworks while already promoting trust by enforcing existing legislation. For example, the Privacy Act, which already protects the use of citizen data in large data sets (an essential element for AI) and is considering measures to improve transparency on the use of Automated Decision Making.

To the extent it is not being done, there is value in reviewing existing regulatory frameworks as they relate to consumer, data protection and privacy, corporate, criminal, online safety, administrative, copyright, and intellectual property laws against the potential harms from AI to determine whether they are fit for purpose. However, this should be done with an:

- understanding of the AI supply chain;
- application of a risk based methodology (see section *Regulatory intervention should take a risk based approach*);
- against set of common principles (see section *Ensure a common set of principles for government AI and the application of regulation*); and
- in a co-ordinated manner (see *A co-ordinating body and governance structure*)

Otherwise, there is a risk that over-prescriptive rules will hinder investments in AI as well as the use of innovative AI solutions.

Are there any further non-regulatory initiatives the Australian Government could implement to support responsible AI practices in Australia? Please describe these and their benefits or impacts.
We consider that there is an opportunity for the Government to play a more active role in the use of AI in the Australian Economy. Governments play a critical role in the safe and responsible economy wide take up of AI as they:

- set and enforce data privacy laws;
- are responsible for large amounts of data;
- are large service providers;
- have IT budgets to deliver major projects; and
- are directly accountable to their citizenry.

Governments have an important role in influencing public attitudes to AI. If governments use AI ethically and responsibly, this will build public trust and acceptance of the use of AI across the economy. The Government must accelerate its use of AI in its systems of operation of government and service delivery.

Do you have suggestions on coordination of AI governance across government? Please outline the goals that any coordination mechanisms could achieve and how they could influence the development and uptake of AI in Australia.
Given the cross sectoral impact of AI technology, co-ordination by government will be critical. This will require new ways of working and potentially cabinet endorsement of a formal approach that will require all government agencies to follow.

At the centre of this would be a government body to ensure no duplication of effort by organisations and individuals, no conflict between policy and legislative proposals, and where avoidance of overlap is not possible clear guidance on which rules should be followed by industry.

In acknowledgement of the independence of regulators – at a minimum the new body would be available to ensure all regulators remained cognisant of approaches being made by other regulators, alert them to potential areas of conflict and how other regulators were applying the principles. This body could also be source of AI understanding and expertise that could support whole of government and regulator understanding of AI and early identification of cross-sectoral emerging issues. This function should however be sub-ordinate to the key function which is to support co-ordination between policy makers and regulators.

Without co-ordination there is a risk of overlapping regulations that will hamper the ability of companies to develop AI-based innovative business models and thereby remain competitive at a global scale.

We are agnostic as to whether a new statutory organisation is required or whether the function of the body could sit within an existing Agency. What is important is that the organisation is empowered to act as a central co-ordinating body across government.

Responses suitable for Australia

Are there any governance measures being taken or considered by other countries (including any not discussed in this paper) that are relevant, adaptable and desirable for Australia?

SAP is supportive of the pro-innovation governance approach of the UK government. This is based on sector specific regulation, linked to cross-sectoral principles that can be tailored to each sector backed by a central agency responsible for regulatory co-ordination and assessment of any cross cutting AI risks.

Target Areas

Should different approaches apply to public and private sector use of AI technologies? If so, how should the approaches differ?

What constitutes responsible use of AI technology should not differ depending on the type of organisation. However, Governments are in a unique position in their use of AI technologies given their role and ability to influence public perception of responsible use of AI. If governments use AI ethically and responsibly, this will build public trust and acceptance of the use of AI across the economy.

How can the Australian Government further support responsible AI practices in its own agencies?

AI offers huge potential benefits for the public sector – such as delivering enhanced citizen services, improving process efficiency, enabling future cities, and ensuring public security and safety. But there have been challenges in its adoption within government processes. We have collaborated with the University of Queensland to investigate how government organisations can break down the barriers for artificial intelligence adoption and value creation.

The first stage of the research identifies the AI challenges for government and develops a high-level framework of capabilities, capacities and processes that are needed to create value from AI while minimizing the risks.

The second stage of the research addresses the specific challenge of 'explainability' of the AI results with an emphasis on aligning AI operations with the stakeholder-specific perspectives and knowledge thus delivering the intended value of the use of the technology.

The third stage examines the specific capabilities required within the public sector to fully realise the value of AI across the organisation.

The fourth stage analyses how to segment and manage the impact of integrating AI within existing work processes.

Further detail and documentation on these stages is available at SAP's Institute for Digital Government[2].

Given the importance of transparency across the AI lifecycle, please share your thoughts on:

a. ***where and when transparency will be most critical and valuable to mitigate potential AI risks and to improve public trust and confidence in AI?***

There is a role for Transparency across the steps AI lifecycle. At SAP we define 5 steps in the AI development lifecycle.

1. **Ideation** – use case identification based on common domain and AI expertise
2. **Validation** – Experiments to assess feasibility
3. **Realisation** – Development of AI functions
4. **Productisation** – Integrating of AI functions into business processes
5. **Operations** – Delivery of embedded AI functions to customers

For the Ideation and Validation phase the following transparency principles are applied

- AI systems interacting directly with humans should be made identifiable as such.
- Prevent misuse of AI system in production.

For the Realisation, Productisation and Operations phase the following principles are applied:

- Data sets and development processes must be documented.
- The AI systems capabilities and limitations must be documented.
- Transparency on how personal data is processed must be provided in alignment with applicable data protection and privacy laws.
- For decisions about affecting humans explanations have to be provide to the data subject.
- The methods used for testing and validation must be documented.

b. **mandating transparency requirements across the private and public sectors, including how these requirements could be implemented.**

Outside of the proposed amendments to the Privacy Act, we do not think that there should be cross-sectoral mandated transparency requirements.

Do you have suggestions for:

a. ***Whether any high-risk AI applications or technologies should be banned completely?***

As a business, SAP prohibits the development of certain AI use cases. These are as follows

Personal Freedom

- Human surveillance – where it is used for targeting individuals or groups with the purpose of disregarding or abusing the rights of individuals or groups.
- Discrimination – where it used to discriminate or exclude individuals or groups from access to AI benefits and opportunities to the wider population

[2] https://discover.sap.com/sap-institute-digital-gov/en-us/publications.html#:~:text=Leveraging%20Artificial%20Intelligence%20in%20Government

- Deanonymisation – where it issued to deanonmysie data anonymised data to result in the identification of individuals or groups.

Society

- Manipulation – where it issued to deceive or unfairly manipulate individuals or groups via public forums, media or moderation of other similar uses.
- Undermine debate – where it is used to undermine human debate or democratic electoral systems.
- Intentional harm – where it is used to intentionally harm users and or those directly or indirectly affected by the system.

Environment

- Environmental harm – all systems shall be conducted with minimum to no explicit damage to the environment.

We do not recommend the Government institute a blanket ban on specific AI technologies. We recommend sectoral reviews to determine the extent to which existing laws would prohibit the use of AI in the manner outlined above. To the extent the laws are silent on this matter the government could consult on the question as to whether additional protections should be in place to protect Australian citizens from the identified harms.

b. Criteria or requirements to identify AI applications or technologies that should be banned, and in which contexts?

As per response above.

What initiatives or government action can increase public trust in AI deployment to encourage more people to use AI?

We consider that there is also an opportunity for the Government to play a more active role in the use of AI in the Australian Economy. Governments play a critical role in the safe and responsible economy wide take up of AI as they:

- set and enforce data privacy laws;
- are responsible for large amounts of data;
- are large service providers;
- have IT budgets to deliver major projects; and
- are directly accountable to their citizenry.

Governments have an important role in influencing public attitudes to AI. If governments use AI ethically and responsibly, this will build public trust and acceptance of the use of AI across the economy. The Government must accelerate its use of AI in its systems of operation of government and service delivery.

This is also critical to good policy making. To make good policies about AI, you need to understand it well. This will only happen with greater use of AI within government. This will allow the government to best appreciate how it works, what the risks are and how to best mitigate them.

SAP's Institute of Digital Government has undertaken research into the use of AI within Government and its challenges. The research has indicated that there are four major challenges facing the government's use of AI.[3]

[3] https://discover.sap.com/sap-institute-digital-gov/en-us/publications.html#:~:text=Leveraging%20Artificial%20Intelligence%20in%20Government

1. **AI is resource intensive** – To effectively utilise AI requires people with the skills to develop and use AI, the systems to undertake the analysis and the data sets on which to undertake the analysis – government agencies face challenges in all those matters.
2. **The right operating model** – Operationalising the use of AI requires new ways of operating – it requires a combination of data science skills along with policy domain expertise in the design and operation of the AI. This requires new ways of operating within typically separate areas within agencies
3. **Opaqueness of AI models -** Many advanced AI systems face the challenge of not being able to be understood by humans, the so called explainability problem This is a particularly a challenge for governments due to the potential ramifications of government decisions on an individual and the importance for governments to be able to demonstrate fairness and transparency in decision making.
4. **Cultural issues** – Perceived and actual impact on employment, challenges to established wisdom and concerns around the public's acceptance of AI within service delivery are all elements that impact on AI take up within the public sector.

AI is ultimately a tool, and its use should result in better business and government operations. If it fails to do so, its adoption within government will face challenges.

Currently, the adoption of AI technologies by businesses and governments is still in its early stages. Use cases are still being developed, and the application of the technology to existing processes is relatively new. This can understandably lead to reticence within government to undertake AI projects where the benefits are unclear or the capabilities are unproven. Like all new technologies, making a business case for their use when the results are unclear or unproven is challenging. Equally problematic is the high expectations on the insights the application of AI can provide, where there is a lack of clear understanding of what the AI can deliver.

However, all these challenges are surmountable, and the Australian Government, in partnership with industry, academia, and community organizations, must embrace AI technologies. We are seeing positive developments across the public sector to help with the growth of AI use. For example, the DATA Act will empower access to greater data sets across the economy. There is also a growing willingness by political leadership to ask how AI technologies can help make the public sector more efficient and deliver better customer services.

Risk-based approaches

Do you support a risk-based approach for addressing potential AI risks? If not, is there a better approach?

Yes. Regulatory interventions should be scaled to meet the risk i.e. an assessment of the likelihood of harm against an individual or organisation combined with the severity of that outcome. For example:

- High Impact High Likelihood - The governance and assessment of an AI system used in an autonomous vehicle would more likely require some form of intervention or governance oversight
- Low Impact Low likelihood – An AI platform used by a business to optimise its inventory management system.

To reflect on the risk-based approach, it is essential to set up a clear and precise criterion for high-risk AI systems based on the probability of occurrence and consequences for individual rights and freedoms, security, or safety and how to mitigate such risks.

Any risk assessment should include assessing the benefits of a proposed AI application or the risks of not proceeding with the development or deployment of the AI application. This is just as important as focusing on the harm that may result from proceeding with the AI application and makes sure the use of an AI application is proportionate to the desired outcomes. There are many high risks with an AI system processing sensitive personal data (e.g. in healthcare) that would be outweighed by the benefits to individuals and society at large from such applications.

To conduct risk mitigation when using high-risk industrial AI applications, international standardisation bodies, driven by industry, should develop common standards for the use of AI in business. Policy makers should seek to advance innovation and promote a risk-based approach to AI that fosters trust, promotes harmonisation of standards, and support global alignment on AI through the OECD and other international for a and work with our allies to advance AI research and development.

The establishment of regulatory sandboxes are also essential for a risk-based approach. Here AI applications can be tested in protected legal environments to develop innovations and regulations with high practical applicability. In addition, joint experimental spaces for AI applications with partner jurisdictions should be pursued.

Is a risk-based approach better suited to some sectors, AI applications or organisations than others based on organisation size, AI maturity and resources?
We recommend that the risk-based approach can be applied across all sectors. The application of regulation should be applied uniformly regardless of an organisations size.

What elements should be in a risk-based approach for addressing potential AI risks? Do you support the elements presented in Attachment C?
Not completely. The proposed framework articulates requirements and obligations that will apply depending on the risks that are assessed by the regulator. When in practice there are a range of possible interventions or requirements that a regulator could consider. The proposed description of what constitutes low medium and high risk appears appropriate.

Should a risk-based approach for responsible AI be a voluntary or self-regulation tool or be mandated through regulation? And should it apply to:

- ***a. public or private organisations or both?***
- ***b. developers or deployers or both?***

The risk-based approach should be used as a model for government to determine if it should intervene on an AI related harm or issue. It should not be a model that becomes a regulatory requirement that is applied on industry.

Any proposed AI related regulation must consider the different roles and abilities of the organisations involved in creating and using AI. The responsibility and consequences of meeting those regulations should fall on the group best able to identify and reduce the risk of harm that made the regulation necessary.

Regulation should reflect the different roles and abilities of the organisations involved in creating and using AI. The responsibility and consequences of meeting those regulations should fall on the group best able to identify and reduce the risk of harm that made the regulation necessary. There should consequently be a distinction made between Developers and Deployers.

The two roles can be distinguished as follows:

- an organisation that designs, codes or produces an AI system, for example a system integrated into an expense management solution to read digital images of receipts is a **Developer**

- an organisation that uses that AI system to make a decision for a customer, employee or for its own business operations is a **Deployer**; and
- in some cases, the same organisation may be both a Developer and a Deployer.

A Deployer using an AI system does not generally have control over design decisions made and data used by the organisation that developed the system. Likewise, a Developer generally does not have control over the subsequent uses of the AI system by an organisation that deploys the system.

It is critical that Deployers have the necessary data governance practices in place to ensure the proper use of AI models provided by developers. Data used in AI applications is specific to the use case and Deployers should understand the associated risk of using poor quality or inaccurate data will have on the AI model's decision making.

AI regulation should make clear the responsibilities and obligations of AI Developers and Deployers. This ensures the appropriate organisation in the supply chain can identify and mitigate risk. Importantly from a citizen or customer perspective it ensures that lines of accountability are matched to the relationship between the end user and provider.

For example, transparency obligations as to the use of AI in high impact decision making would be best applied to the Deployer as they have a direct relationship with the customer whereas the Developer will have no relationship with the customer.

This distinction has parallels to the General Data Protection Regulation (**GDPR**), widely considered to be best practice privacy regulation which has the Processor / Controller distinction. The benefit of this distinction was recognised in the context of the *Privacy Act 1988* (Cth) ('Privacy Act') reforms which recommend amendments to the Act to incorporate the Processor Controller distinction.

Furthermore, a distinction can also be made between scenarios which involve direct interaction with consumers or citizens and business to business interactions. In the business-to-business context we would recommend a maximum freedom to contract to establish responsibilities and obligations on the entities best placed to comply with them and mitigate risks and understand the specific context and use-case.