JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

INQUIRY INTO COMMONWEALTH FINANCIAL STATEMENTS 2022-23

ANSWERS TO QUESTIONS ON NOTICE

Agency: Australian Taxation Office
Reference: Written
Topic: Use and Governance of AI Systems in the APS
Senator: Julian Hill MP

Question:

1. For what purposes do you currently use AI in your entity, and do you have planned or likely future uses? Please summarise.
2. Which legislative, regulatory and policy frameworks (including cross-Government policies) are relevant to your entity's use of AI?
3. What are your internal framework/policies for assessing the risks associated with the use of emerging technologies such as AI, specifically in the areas of security, privacy, ethics, bias, discrimination, transparency and accountability?
4. What are the supply chain risks when using existing AI solutions or software?
5. What additional controls been developed by your entity to manage:
    a. the broad risks associated with AI
    b. the risks associated with the design and implementation of systems using AI
    c. the risks associated with change management policies that arise from the use of AI
6. How do you manage regular updates to AI and supporting data?
7. What considerations or planning do you undertake for any additional capability required to implement AI?
8. What frameworks have you established to manage bias and discrimination in any of your systems that use AI?
9. How do you ensure that that the use of AI meets government security and privacy requirements?
10. What briefings are given to your audit and risk committees, or boards, on the use of AI?
11. How does your internal audit program consider the robustness of controls for AI to provide assurance around mitigation or risks?
12. As part of your system design process, how do you audit and trace the output of, and decisions made through, AI?
13. Are the AI platforms in use at your entity:
    a. off the shelf products
    b. customised from other products
    c. systems developed in-house?
14. Who has ownership and possession of the source code for your AI, and can you understand this code, including its capacity to learn and innovate? How?

Answer:

1. The ATO uses AI tools to increase the efficiency and effectiveness of work done by staff enabling us to deliver better services and greater value to the community. The ATO currently uses AI to review large quantities of unstructured data for risk and intelligence purposes, power risk models to identify potential non-compliance for human review, and draft and edit

communications. The ATO has human oversight over all uses of AI, and decision making that impacts clients is always made by a human.

The ATO is also part of the Government's Microsoft Co-pilot for Microsoft 365 trial. Use cases being explored include content summarisation, notetaking and slide creation. The findings from the trial will help inform the ATO's future use of Co-pilot for Microsoft 365.

Note, the ATO considers AI to include machine learning, deep learning and generative AI. The ATO considers rules-based analytics to be separate to AI.

2. The ATO adheres to all AI-related legislative, regulatory and policy frameworks in its use of AI. These include those issued by the Digital Transformation Agency (e.g. Artificial Intelligence policy and the Interim guidance on Generative AI for Government agencies) and those issued by other agency (e.g. the Commonwealth Ombudsman Automated Decision-making Better Practice Guide).

In any use of AI, the ATO applies all standard laws and frameworks. This includes complying with laws governing tax, superannuation and business registration, the Privacy Act 1988, Privacy (Australian Government Agencies – Governance) APP Code 2017, Archives Act 1983, and aligning with the Commonwealth Risk Management Policy.

3. Frameworks and policies the ATO uses to assess risks with use of technologies, including AI, are:

- A security approval to operate (SATO) assesses the security risk of the new technology and ensures the safety of ATO systems and data. A SATO is required before any new technology is brought into the ATO IT environment.
- Privacy impact assessments for high privacy risk projects, adhering to the Privacy (Australian Government Agencies – Governance) APP Code 2017.
- Data ethics threshold assessment is undertaken when commencing data and analytics activities, including those using AI. Depending on the outcome, a more detailed impact assessment may be required.
- *Use of publicly available generative AI technology* policy (issued in December 2023) outlines the process for assessing risks of new publicly available generative AI technologies and uses of them. This policy aligns with the Interim guidance on Generative AI for Government agencies.

4. When using existing AI solutions or software, the supply chain risk is similar to any other software product including issues of quality and performance, data privacy and security, bias and transparency, vendor lock in, third party (i.e. risks of an adverse event by using software supplied by a third party), legal and regulatory, and financial (e.g. the supplier could cease support due to insolvency or other reasons). Out of support software may result in undetected or unpatched vulnerabilities as well as interoperability or compatibility problems with other parts of the broader system.

5a. The ATO Data ethics principles help to address some of the risks associated with use. The ATO has also made available to all staff learning products on AI, including a foundation product on generative AI. Increasing the data literacy of all staff is a key control for ensuring data and analytics, including the outputs of AI, are used appropriately and effectively and to reduce the risk of any misuse or negative impacts.

5b. The ATO's use of AI is always within the context of a broader system or program to address a particular behaviour or deliver a particular service to clients. The ATO uses well

established management approaches, including program and project management and risk management, to ensure the work programs and systems it designs deliver the intended benefits and any risks are identified and appropriately managed.

5c**.** The ATO has significant experience in managing change related to the introduction of new technologies, including where the new technology impacts its entire workforce or large portions of its clients. It has established processes in place and support material for staff in managing change. The ATO has not seen the need to introduce any additional controls to manage change management risks associated with the use of AI over and above the existing controls and processes.

6. The ATO manages regular updates through system version controls and detailed documentation for both models and data to track changes and ensure repeatability. The ATO has also developed clear data governance policies to ensure data quality, integrity and security throughout the update process. The ATO also has processes to monitor model performance.

7. The ATO has a well-established approach to planning for additional capability required to implement any new technologies, legislative requirements or respond to changes to the external operating environment. The ATO has also approached capability building for the implementation of AI from the perspective of staff as users (majority of staff) and staff as developers of AI solutions (staff in IT and data and analytics professional roles). Capability development programs are tailored to each cohort.

8. The ATO has a Data Ethics Framework to assess potential issues with the use of data, including bias and discrimination. The framework covers all uses of data, including through AI. The data ethics assessments and privacy impacts assessments referred to in response to question 3 are part of the Framework and help to manage bias and discrimination in systems that use AI.

9. AI is used in line with existing ATO security and privacy policies, as per response to question three. These policies comply with government requirements.

10. There are no regular briefings provided to committees specifically on the use of AI, but ad hoc briefings are provided as requested. AI is covered under the ATO's enterprise risks *Misuse of data and analytics* and *Maximise the value of data and analytics*. Briefings on the management of these 2 risks are provided to the ATO internal Risk Committee annually.

11. The ATO Internal Audit team has considered AI as a component of other reviews and will continue to do so in future reviews, where relevant.

12. The ATO has the following processes to audit and trace the output of an AI system to ensure transparency, accountability, and performance:

- logging and metadata collection – record all input data, processing steps and outputs systematically. Collect metadata including timestamps, data sources and pre-processing steps to provide context for each dataset (data catalogue).
- model documentation – document model specifications including model architecture, algorithm used, the rationale for choosing the algorithms, and model training details and model parameters.
- version control – a version control system to store code and maintain model versions.
- audit trails – maintain detailed logs of all operations, decisions and changes made to the system.

13. The AI platforms in use or reviewed for use in the ATO range from off the shelf products through to systems developed or integrated in house. This includes the ATO's participation in the whole-of-government trial of Microsoft 365 Co-pilot, coordinated by the Digital Transformation Agency.

14. The ATO has a group of specialist data scientists who are developing the AI models and process the source code of the AI tools used in the ATO. As such, the ATO has ownership and possession of the source code for the AI models it uses. The team have significant skills and knowledge in required areas including programming, machine learning and deep learning, and experience in model development, validation and deployment. Therefore, they understand the source code they are using and how the models are trained and learn.