Joint Committee of Public Accounts and Audit
Inquiry into Commonwealth Financial Statements 2022-23

QUESTION ON NOTICE

Outcome: Corporate and Enabling Services

Department of Employment and Workplace Relations Question No. IQ24-000032

The Hon Julian Hill MP, provided in writing 20 May 2024

20 MAY 2024* | *WRITTEN QoNs from Chair Julian Hill MP* | *AI Governance

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. **For what purposes do you currently use AI in your entity and do you have planned or likely future uses? Please summarise.**

The department currently has restricted the use of generative AI products on its IT network and participated in the whole of government Microsoft Co-Pilot trial.

The department has established an innovation capability to test AI and other emerging capabilities to better understand AI, the risks and potential benefits. The department is aligning all testing of AI to the current advice from the Digital Transformation Agency (DTA).

2. Which legislative, regulatory and policy frameworks (including cross-Government policies) are relevant to your entity's use of AI?

DEWR's use of AI is governed by multiple legislative, regulatory, and policy frameworks, including DTA's guidance for APS staff on the use of Generative AI, Australian Privacy Principles under the *Privacy Act 1988*, the Protective Security Policy Framework, the Information Security Manual (ISM), the Hosting Certification Framework, the *Fair Work Act 2009* and the department's enterprise agreement and the *Work Health and Safety Act 2011*.

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?

The department has internal Generative AI Guidelines which are based on the DTA Interim Guidance. We are also developing an internal data and ethics assessment process.

The department manages AI within our existing technology management processes. This includes following cyber security controls and privacy controls for all ICT technologies and capabilities.

4. What are the supply chain risks when using existing AI solutions or software?

The department views the supply chain risks for AI similar to other ICT technologies, such as the location of data it stores, who has third party access and the sovereign ownership of the technology.

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

The department has set up an innovation process to contain and manage our exploration with AI. We are also part of the AI whole of government taskforce and are working on an internal data and ethics assessment process to ensure that our AI system design aligns with ethical and security standards.

6. How do you manage regular updates to AI and supporting data?

The department manages AI like any other ICT product within our software delivery lifecycle, ensuring proper version control and management. Regular updates are handled through our established processes, including scheduled maintenance.

7. What considerations or planning do you undertake for any additional capability required to implement AI?

The department adheres to all whole of government advice and policies. The department is actively engaging with the AI taskforce (led by the DTA and DISR) and will implement any procedures or policies. Additionally, we continue to develop our internal AI capability and understanding through our innovation process, ensuring that we are equipped to effectively implement and manage AI technologies.

8. What frameworks have you established to manage bias and discrimination in any of your systems that use AI?

The department is developing an internal data and AI ethics process to ensure comprehensive management of bias and discrimination in our AI systems. We align with the DTA's advice and adhere to 'human in the loop' principles. We have also leveraged the NSW assurance framework for AI to help assess risks for our innovation proof of concepts.

9. How do you ensure that the use of AI meets government security and privacy requirements?

All ICT capabilities within the department are reviewed and authorised to operate prior to use in accordance with the PSPF and ISM.

10. What briefings are given to your audit and risk committees, or boards, on the use of AI?

The department provides updates on our use of AI to our Audit and Risk Committee.

11. How does your internal audit program consider the robustness of controls for AI to provide assurance around mitigation or risks?

The department's current internal audit program includes a range of activities that focus on the cyber security, information management and general IT controls, which all contribute to the management and assurance of AI within the department.

12. As part of your system design process, how do you audit and trace the output of, and decisions made through, AI?

The department does not have any AI driven automated decision-making capabilities. Our current AI exploration ensures human in the loop principles to manage and assess AI output. AI is integrated as one component within a broader IT environment, ensuring robust data management, application control and access control.

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.

AI is a very large umbrella term for a variety of different technologies. The department's software providers, such as Microsoft, are providing AI services which we are trialling as part of the whole government co-pilot work. We are also working on building internal capability to better understand and leverage AI.

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?

The department treats AI like other ICT capabilities and technologies developed, as such follows our existing processes around ownership and control. The department does not build or leverage any Artificial General Intelligence (AGI) capacities with the ability to self-learn.