Our insights

Using artificial intelligence

Recent years have seen rapid growth in artificial intelligence (AI) and large language models (LLMs) like ChatGPT and Microsoft Copilot. While AI offers significant potential to transform the public sector, SA Government agencies mustbalance innovation with accountability, transparency, and public trust. The challenge lies in building the expertise, systems, and governance needed for safe adoption while developing the capability to assess AI applications and their controls.

The SA Government is encouraging agencies to use AI as a tool for efficiency, data insights and service improvement. The Office for AI was established in July 2024 to help build central AI capabilities and oversee the allocation of the AI Proof of Value Program funding. $28 million was allocated in the 2025-26 State Budget to the Digital Investment Fund for the AI Program across the public sector. It states that its first priorities are transcript initiatives being developed with the South Australia Police and SA Health to help efficiently share accessible information across government.

Risks

Integrating AI into government services carries significant risks that must be managed to maintain public trust. Poor or incomplete data can lead to bias and unfair outcomes, while AI-driven decisions raise privacy concerns and require transparency and oversight to uphold equity and accountability.

Operational challenges include legacy IT systems, automation bias, and cybersecurity vulnerabilities, all of which threaten reliability and service continuity. The complexity of AI technologies also creates audit challenges, requiring ongoing assessment and guidance on governance.

As AI adoption grows, we will monitor its use and incorporate AI risks into future audit programs.

Overview of agency AI use in 2025

In July 2025 we surveyed 23 large SA Government agencies. We found that most of these agencies have developed central guidance to support the use of AI and are aware of the importance of good governance.

Current use

Most agencies are in the early or exploratory stages with AI.

AI use is generally limited to pilots, productivity tools or embedded features in commercial software.

Most agencies are involved in the whole-of-government Copilot trial.

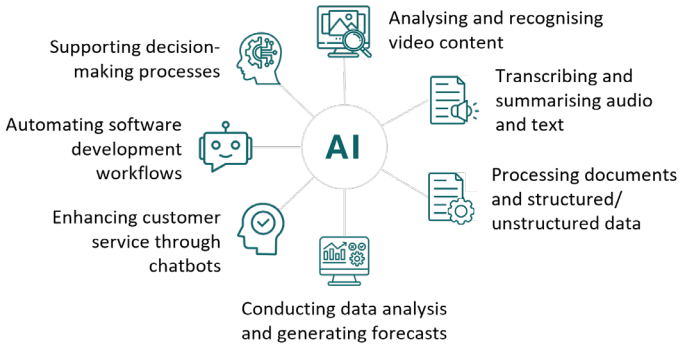
Most agencies are not yet using AI for core decision-making. AI is generally used as a support tool, with final decisions made by staff.

Planned or experimental use

Many agencies are expanding their AI pilots or proof of concepts, especially for document analysis, chatbots and workflow automation.

Planned uses target efficiency, data insights and reduced administrative burden.

Some agencies are planning to delegate meaningful decision-making to AI in the near term.



Challenges and maturity

Agencies are keen to innovate but remain cautious about delegating critical decisions to AI.

AI is used as a support tool, with people still responsible for final decisions.

Agencies noted the fast pace of AI development and the need for ongoing review and adaptation. This includes the increased prevalence of AI features in standard software that requires vigilance and policy updates.

Articial intelligence governance

Governance and risk management

Many agencies have established or are forming AI governance committees or working groups. Agencies advised us that they align with the Office of the Chief Information Officer (OCIO) AI guidelines, with their individual policies being developed or updated based on State and Commonwealth Government guidelines.

Their AI policies emphasise fairness, prevention of bias, privacy, and compliance with legal and ethical standards, and mandate staff training and stakeholder engagement to ensure its responsible use. Agencies also require documentation, risk assessments and clear reporting when AI is used.

South Australian Cyber Security Framework and guidelines for using AI

The *South Australian Cyber Security Framework* is a mandatory policy that requires all SA Government agencies to have cyber security policies and procedures in place and approved by their senior leadership. This includes a policy governing the safe selection and use of generative AI and LLM tools.

The *Guideline for the use of Generative Artificial Intelligence and Large Language Model Tools*, written by OCIO, applies to all SA Government agencies, people and non-government suppliers accessing government resources.

Elements of governance to support the use of AI technologies

Adopting AI technologies in government must be underpinned by robust governance to ensure that risks are appropriately understood and managed. AI good governance involves:

Governance and leadership

Establish clear goals, roles and responsibilities for AI initiatives.

Ensure alignment with public values, including fairness, transparency and accountability.

Promote ethical oversight through appropriate governance.

Performance and reliability

Define measurable performance metrics and regularly evaluate AI systems against them.

Conduct risk assessments and scenario testing to identify potential failures or biases.

Ensure systems are resilient, adaptable and able to be maintained.

Data integrity and privacy

Use high-quality, representative and secure data to train and operate AI systems.

Implement robust data governance policies to protect privacy and prevent misuse.

Ensure transparency in data sourcing and consent mechanisms.

Monitoring and accountability

Continuous oversight through audits, evaluations and public reporting.

Enable redress mechanisms for individuals affected by AI decisions.

Clarify legal accountability for AI outcomes, including liability and the ability to track decision-making.

What agencies should do

Establish AI governance frameworks

Define roles, responsibilities and ethical oversight.

Align with OCIO guidelines and South Australian Cyber Security Framework.

Invest in capability building

Train staff on responsible AI use.

Engage stakeholders to build trust and transparency.

Prioritise data integrity and privacy

Use high-quality, representative datasets.

Implement robust data governance and consent mechanisms.

Monitor and audit continuously

Set measurable performance metrics.

Enable redress mechanisms for individuals affected by AI decisions.

Develop risk management processes

Conduct bias testing, scenario analysis and cybersecurity assessments.

Require documentation and clear reporting for all AI use.

Find out more at audit.sa.gov.au

Source: Audit Office of South Australia, *Auditor-General's Report 8 of 2025 Annual report for the year ended 30 June 2025, Part A: Executive summary*, published June 2025.

Government of South Australia
Audit Office of South Australia