Australian National Audit Office

Governance of Data

Insights: Audit Lessons

Introduction

The aim of Audit Lessons is to make it easier for the Australian public sector to apply insights from our audit work.

Governance of Data is targeted at Australian Government officials in information governance roles and those who use data to achieve organisational objectives.

Data is any information in a form capable of being communicated, analysed or processed (whether by an individual, a computer or other automated means).[1] Data becomes valuable when it is processed and analysed to extract meaning, leading to insights, decisions or predictions. *Governance of Data* considers structured data that is measurable, such as a set of observations organised into a table, spreadsheet or database — in contrast to unstructured data that cannot be easily measured, such as records of meeting minutes.

Data is a valuable asset of every Commonwealth entity, as it underpins informed decision making, efficient and effective business operations and public accountability. This means entities should invest in its governance, quality, security and ethical use to ensure data is trusted, protected and used to drive measurable results and outcomes for citizens.

Effective governance of data is critical to realising and maximising the economic, social and environmental benefits of data. This includes securely, safely, lawfully and ethically sharing data with other public sector jurisdictions, in accordance with the Intergovernmental Agreement on data sharing between Commonwealth and State and Territory governments.[2] Good data governance is also necessary to meet legislative obligations and policy.

Through its audit work, the ANAO has observed good practices and fundamental deficiencies in the governance of data across multiple entities. Governance deficiencies have resulted in weaknesses to data integrity (reliability and verifiability), which impacts business processes and can result in reduced capability to make informed decisions, meet reporting requirements and achieve business objectives. Good data governance is essential in analytics, artificial intelligence (AI)[3] and machine learning[4], to ensure ethical use of data, including avoiding bias in AI models.

1 Department of Finance, Senior Executive Service Accountabilities for Data, Finance, Canberra, available from https://www.finance.gov.au/government/public-data/public-data-policy/ses-accountabilities-data [accessed 23 June 2025].

2 The agreement includes application of data sharing principles from the *Data and Availability and Transparency Act 2022*, refers to governance of Indigenous data by reference to the National Closing the Gap Priority Reform 4, and includes the Data and Digital Ministers' Trust Principles.

3 The Australian Government follows the Organisation for Economic Co-operation and Development definition of an AI system: 'An AI system is a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.'

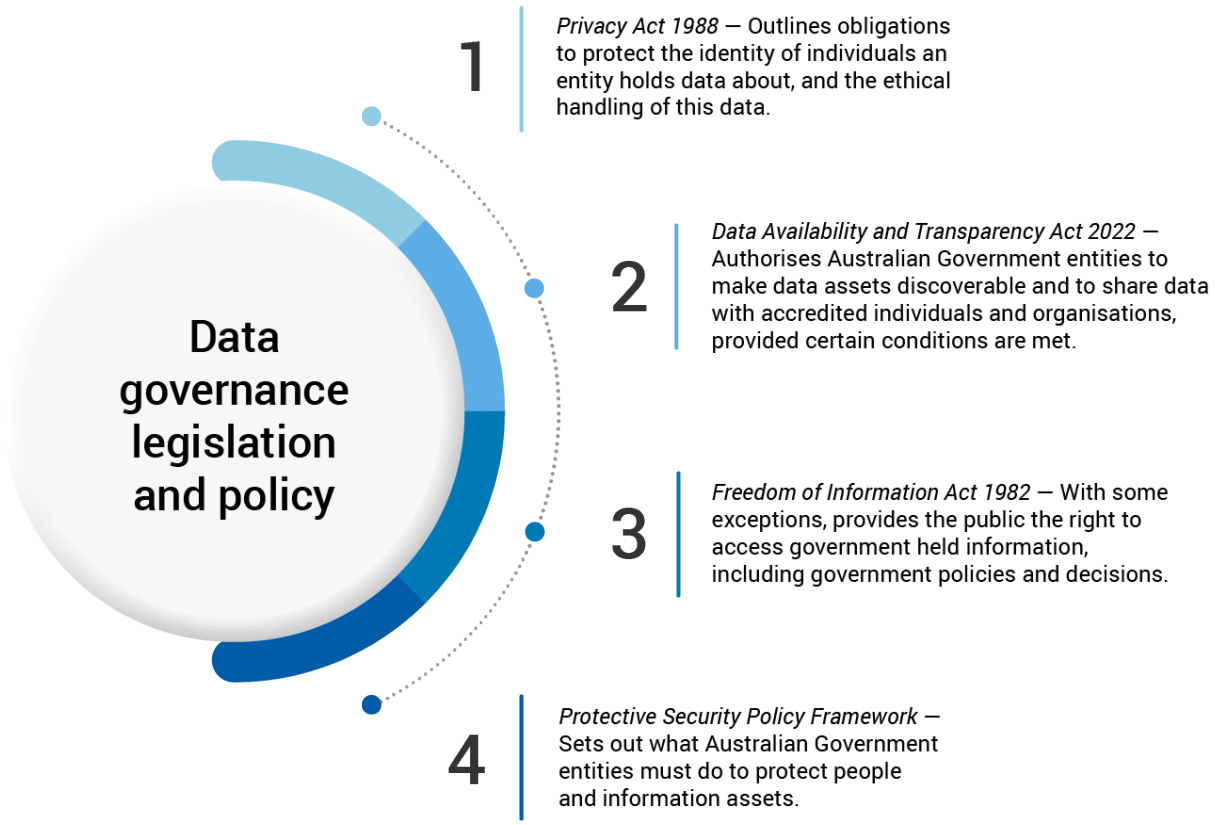
4 The Digital Transformation Agency defines machine learning as: 'a field within AI and computer science dedicated to using data and algorithms to help AI mimic human learning, thereby enhancing its precision over time.'

Benefits of good data governance

- Improved capability to achieve business outcomes.
- More robust evidence base for improved decision making and increased public trust.
- More consistent, coordinated, accessible and timely services.
- More informed policy development and decision-making.
- Better reporting and assurance to the Parliament.
- Improved information exchange and transparency.
- Greater operational efficiency and cost-effectiveness.
- Reduced impact of machinery of government and other business continuity changes.
- Better understanding and management of regulatory and other risks.
- Compliance with legislative requirements, including privacy.
- Increased physical, information and personnel security.

Commonwealth legislation and policy on data governance

Key legislation and policy relevant to data governance



Also relevant are the:

- *Archives Act 1983*, which makes National Archives of Australia responsible for identifying the archival resources of the Commonwealth (that is, Commonwealth information of enduring value), and preserving and making publicly available the archival resources of the Commonwealth;
- National Archives of Australia's *Building trust in the public record* policy, which identifies key requirements for managing Australian Government information assets, including records, information and data; and supports improvement in performance management of public sector data and the use and reuse of data;
- the Department of Finance's *Data Ethics Framework*, which provides Australian Public Service (APS) guidance on ethical use of public data and analytics;
- the Australian Public Service Commission's *APS Data Capability Framework*, which outlines 26 data-specific capability areas associated with working with data in the APS; and
- the Digital Transformation Agency's *Framework for the Governance of Indigenous Data*, which aims to provide Aboriginal and Torres Strait Islander people greater agency over how their data is governed within the APS so government-held data better reflects their priorities and aspirations.

Whole-of-government data strategy

Launched in December 2023, the Australian Government's Data and Digital Government Strategy (the Strategy) aims to provide a blueprint for the use and management of data and digital technologies by the APS through to 2030. The Strategy recognises data as a valuable national asset in realising Australia's economic and social objectives, and in improving the evidence-base for government policy decisions, with a goal of better outcomes for all people and business.

To support implementation of the Strategy, and to help entities self-assess their data maturity over time, the Department of Finance developed the Data Maturity Assessment Tool (DMAT). The self-assessment enables entities to:

- track their data maturity progress over time;
- identify data management strengths and weaknesses; and
- improve their ability to meet reporting obligations for promoting accountability and public trust.

ANAO findings and observations on the governance of data

Performance statements audit

The ANAO provides independent assurance to the Parliament that an entity's annual performance statements meet the relevant requirements of the *Public Governance, Performance and Accountability (PGPA) Act 2013* (PGPA Act) and PGPA Rule. An object of the PGPA Act is to require Commonwealth entities to provide meaningful performance information to the Parliament and the public. Performance statements audits contribute to this objective. Meaningful performance information is based on relevant, reliable, accurate and timely data. It supports evidence-based policy and an entity's strategic planning, budgeting, monitoring and evaluation processes.

Meaningful performance information demonstrates transparency and accountability in an entity's effective stewardship of public resources, contributing to public trust and confidence in government.

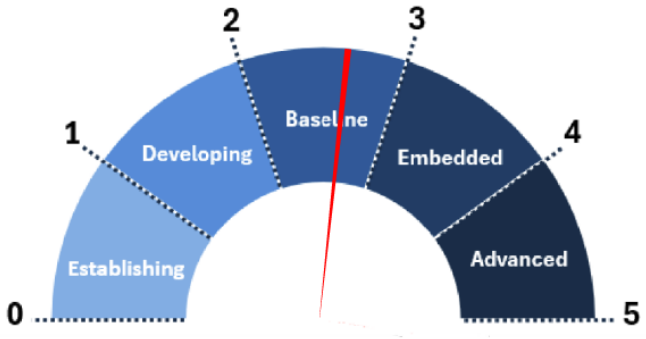
Performance Statements Auditing in the Commonwealth — Outcomes from the 2023–24 Audit Program presented assessment of the performance reporting maturity of 14 Australian Government entities. Performance reporting maturity was assessed across five categories, including 'data and systems', on a scale from zero to five, with five indicating an advanced level of maturity.[5] The average maturity rating for the 14 entities was 2.6 (Baseline) with only one entity assessed as 'Advanced' — the Treasury.

Data and systems maturity across 14 audited entities, 2023−24

Data and systems maturity

'to produce high quality performance information on a consistent basis, entities require information technology systems and processes that can generate complete, accurate and timely data'

Data and systems maturity increased from 2.4 in 2022−23 compared with 2.7 in 2023−24 for repeat auditees



There were improvements to coordination and understanding between specialised data teams and those responsible for policy, service delivery and governance.

Data and systems was the least mature category for all auditees

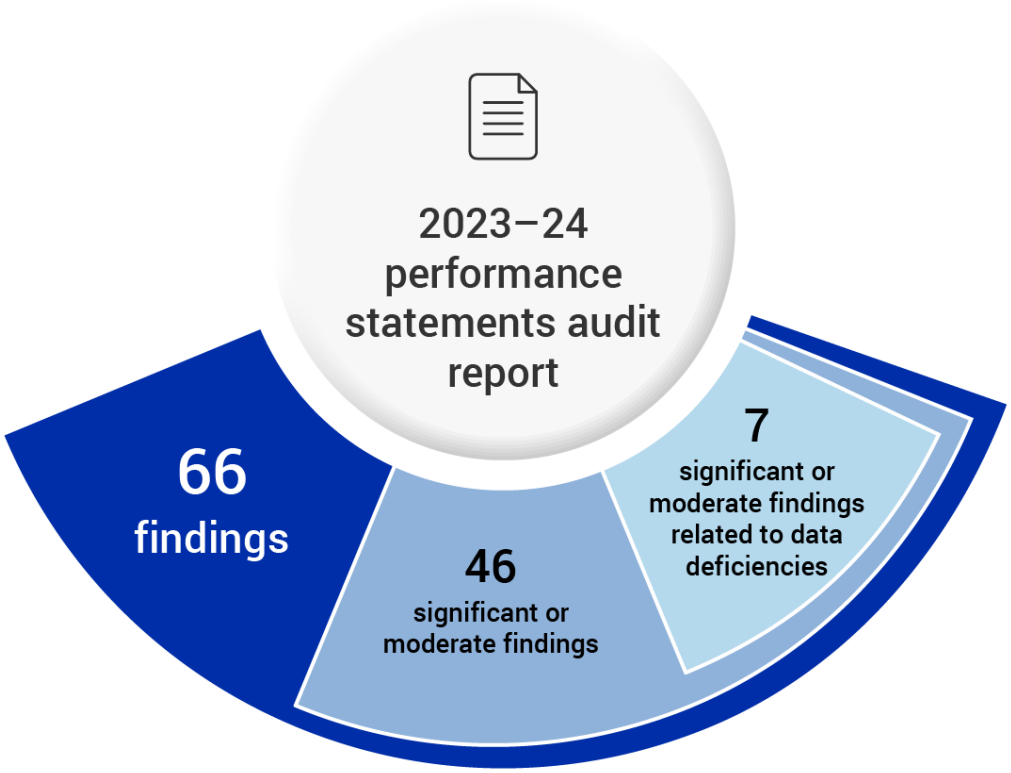
Maturity category	Leadership and culture	Governance	Data and systems	Capability	Reporting and records
Average	3.3	3.1	2.6	3.0	2.8

Most of the 14 entities required significant progress on data governance and assurance in the context of performance reporting.

5 The ANAO's assessment was specific to performance reporting from an audit perspective and is separate but complementary to the DMAT.

The report identified 'data' as one of five themes that emerged from examination of significant and moderate findings.

Findings of the 2023–24 performance statements audit report



Data deficiencies were due to:

- inadequate assurance over data extraction and reporting;
- a lack of controls over how data was managed across the data lifecycle, from data collection through to reporting;
- weak assurance over the accuracy and reliability of data generated and reported by third parties; and
- insufficient documentation, including on data ownership, and on the reliability and verifiability of data and methodologies supporting performance measures.

Entities with data deficiencies tended to exhibit more than one type of weakness in data governance practices.

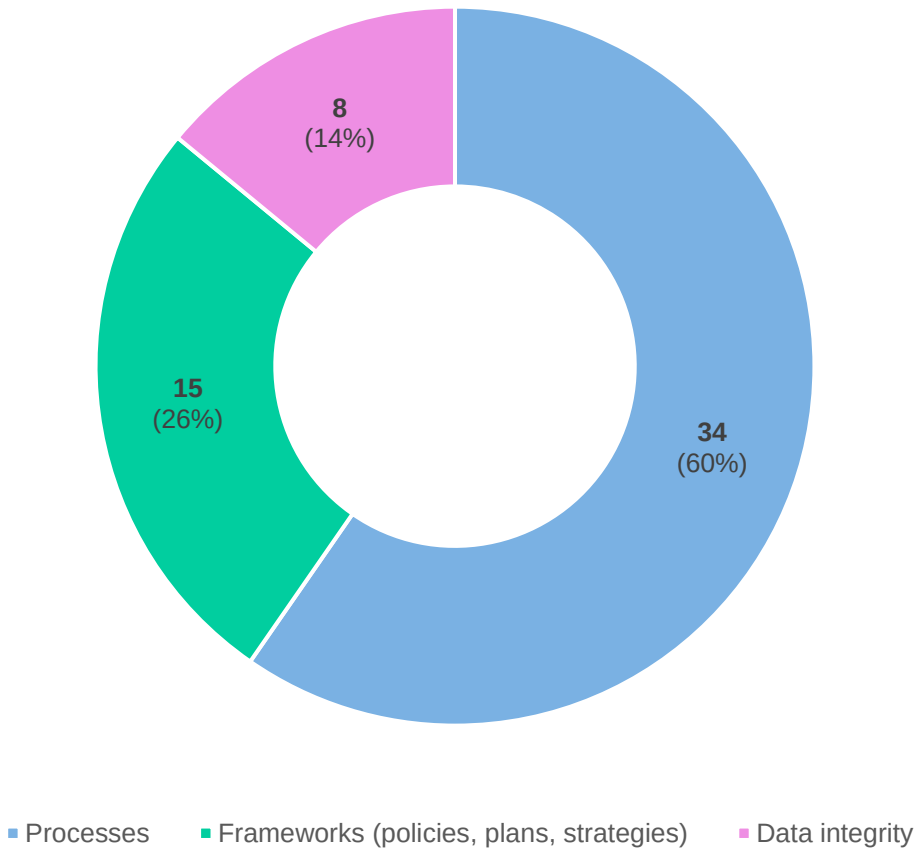
Performance audit

Performance audits provide independent assurance to the Parliament of the operational performance of entities across the public sector.[6] Between 2019–20 and 2023–24, the ANAO

6 The ANAO's performance audit activities are explained in the Insights: Audit Practice product *Performance Audit Process*.

made 857 recommendations in performance audit reports. Of these, 57 (7 per cent) related to the governance of data, including to address weaknesses in data processes and frameworks.

Data governance recommendations in performance audits, 2019–20 to 2023–24



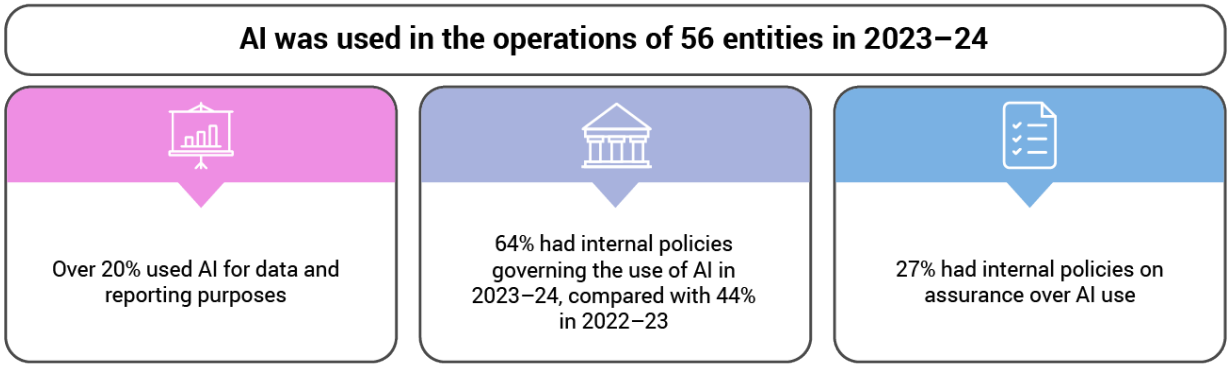
Financial statements audit

The ANAO audits annual financial statements to provide the Parliament with independent assurance of the financial performance and position of all Australian Government entities.

Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2024 noted:

- IT control weaknesses increased risks of unauthorised access to systems and data, or data leakage;
- challenges with assurance over third-party data, especially in relation to cloud computing arrangements (see Case study 7); and
- increased use of AI across the public sector, from 27 entities in 2022–23 to 56 in 2023–24.

Observations on AI use from the 2023–24 financial statements audits



Audit lessons

Governance of Data sets out five lessons aimed at improving data governance practices as part of a broader information management framework in Australian Government entities. These lessons are based on insights drawn from recent ANAO audits and are intended to help entities to realise the benefits of good data governance.

- Lesson 1: Value data as an asset
- Lesson 2: Develop an information governance framework and data strategy
- Lesson 3: Establish data leadership and define roles and responsibilities
- Lesson 4: Document data methodology with data processes mapped end-to-end
- Lesson 5: Strengthen assurance over third-party data

The further reading section provides links to relevant ANAO, Department of Finance and other resources, and additional Insights products.

Lesson 1: Value data as an asset

Entities that value data as an asset are well positioned to make evidence-based decisions and realise the economic, social and environmental benefits of good data. Treating data as an asset means investing in its governance, quality, security and ethical use.

In a culture where data is valued as an asset:

- there are clear data governance frameworks, policies and strategies, which are aligned with the whole-of-government Data and Digital Government Strategy;
- there is leadership commitment, including a sole authority (such as a Chief Data Officer or equivalent data leadership role) responsible for all entity data, whose role includes fostering a culture where data assets are valued — they may work with a team with defined data roles and responsibilities to oversee data governance and practice;
- there is an entity culture that values curiosity, evidence and continuous learning from data;
- the data that is required to achieve business objectives is considered from the outset;
- data is collected and used with a purpose, such as for evidence-based policy, and to evaluate and measure performance;
- instead of selecting and designing systems around existing data that is not actually fit for purpose, systems are selected and designed based on required data outputs;
- there is clear methodology documentation (such as standard operating procedures and workflows) that enables users to easily locate and understand required data at any point in a process;
- appropriate controls are in place to assure the integrity of data, such as regular data checks and sign off by senior staff certifying data quality and integrity;
- emerging technologies are used responsibly to improve service delivery and performance;

- staff data capability is uplifted through learning and development programs; and
- data maturity is assessed regularly.

Data maturity assessments support entities in treating their data as an asset. The Data Maturity Assessment Tool developed by the Department of Finance to helps entities periodically measure their data maturity and capability across seven focus areas:

- Strategy and Governance;
- Architecture;
- Operations;
- Risk;
- Quality;
- Reference and Metadata; and
- Integration and Analytics.

Case study 1. A data-first approach

The Australian Maritime Safety Authority (AMSA) managed a contract with Cobham SAR Services (Cobham) for the provision of dedicated airborne search and rescue services. AMSA collected data on the contracted services that Cobham delivered from the outset. It implemented arrangements to ensure the quality and integrity of that data, which demonstrated how AMSA valued data as an asset in its approach to contract management. AMSA's arrangements and its use of available data to establish clear performance expectations contributed to the ANAO's finding that AMSA's management of the contract was fully effective.

- ✓ AMSA created a bespoke IT system to capture data on Cobham's contractual performance requirements and related payments. Data on operational activities was linked to contractual performance requirements while payments were tied to the achievement of key performance indicators.
- ✓ The data was shared with AMSA contract administrators and Cobham, which supported efficient and effective contract management.
- × AMSA's experience contrasts with the Department of Home Affairs' (Home Affairs) data handling in relation to its contract with Surveillance Australia, which is a subsidiary of Cobham:
  - Home Affairs did not maintain high-quality data that was accurate and complete;
  - key aspects of the contracted service level agreement were not linked to the achievement of performance indicators that determined the amount of monthly payments;
  - a system was not established to capture accurate and complete data to assess contractor performance and transparently calculate related payments; and
  - Surveillance Australia's data did not consistently align with Home Affairs' data, enabling Surveillance Australia to negotiate the mission scores that were used to calculate performance assessments and related payments.

The ANAO recommended that Home Affairs adopt AMSA's approach of using appropriate systems and processes that link operational activity data with contractual performance requirements.

To read more, see key messages and paragraphs 1.8–1.10 of Management of the Search and Rescue Aircraft Contract; and paragraphs 4.1–4.4 and 4.48–4.55 of Management of the Civil Maritime Surveillance Services Contract.

Lesson 2: Develop an information governance framework and data strategy

Good outcomes are underpinned by good data, which is supported by a well-designed information governance framework and data strategy. An information governance framework describes how to value an entity's information assets (records, information and data) across the organisation, with established oversight structures and mechanisms. In relation to data, the framework should:

- provide an overview of the entity's data assets and data management approach to achieve business goals;
- ensure the enduring quality and discoverability of data; and
- apply consistent enterprise-wide standards, policies and procedures for the storage and use of data, regardless of what systems are used by different teams.

A data strategy is a plan that aligns with the information governance framework and the whole-of-government Data and Digital Government Strategy. It should describe the approach to data creation, capture, collection, management and use of data in the context of business objectives. This includes considering data measurement, monitoring and evaluation.

An information governance framework may set out:

- drivers for data requirements, such as legislation, risk and business needs;
- the environment within which data is created and/or captured, collected and managed;
- the principles that guide data design, capture, management and use in the entity;
- roles and responsibilities, including leadership, as they relate to data;
- consistent use of terminology and nomenclature across systems within the organisation and with other entities;
- controls to protect against risks to data and to preserve the integrity of data (this includes IT controls to, for example, restrict access to entity data[7]);
- ethical considerations embedded into data and AI policies;
- senior management commitment to uphold data governance; and
- actions the organisation will take to embed information governance into its culture, such as training and guidance for staff.

7 For more information on IT controls in relation to separating personnel, see the Insights: Audit Lessons product on Management of ICT System Access: Separating Personnel.

With regard to implementing the information management framework, relevant procedures and policies, including an entity's information management policy, should be developed or updated to align with the framework.

Case study 2. Governance processes over lessons learned in Defence

The ANAO conducts an annual review of the Department of Defence's (Defence) major equipment acquisitions. The annual review involves examination of 'Project Data Summary Sheets' that Defence prepares for selected major equipment acquisition projects. Project Data Summary Sheets must follow guidelines endorsed by the Joint Committee of Public Accounts and Audit, which include disclosing lessons learned. Lessons learned are intended to be incorporated into future policy and practice, and are based on data stored in a Defence 'Lessons Repository'.

- × There were deficiencies in Defence's governance processes over lessons learned in their Project Data Summary Sheets.
  - In 2022–23, the ANAO found that lessons learned in the Project Data Summary Sheets and associated data were materially inconsistent with obtained evidence. Defence subsequently advised that preparation of the Project Data Summary Sheets was aligned with internal policy instead of the Joint Committee of Public Accounts and Audit's guideline reporting requirements. This issue contributed to the repeat finding of material inconsistency in the 2023–24 reporting year.
  - In 2023–24, the ANAO identified weaknesses in systems control for data input, data manipulation and data output within the Lessons Repository, upon which Project Data Summary Sheets rely.

The ANAO noted that quality preparation processes for Project Data Summary Sheets would reduce the risk of untimely and/or inaccurate reporting and would reduce the incidence of multiple reviews for the same project.

To read more, see paragraphs 1.10–1.13 of 2022–23 Major Projects Report; and paragraphs 1.16–1.18 and 1.94, and Part 2 of 2023–24 Major Projects Report.

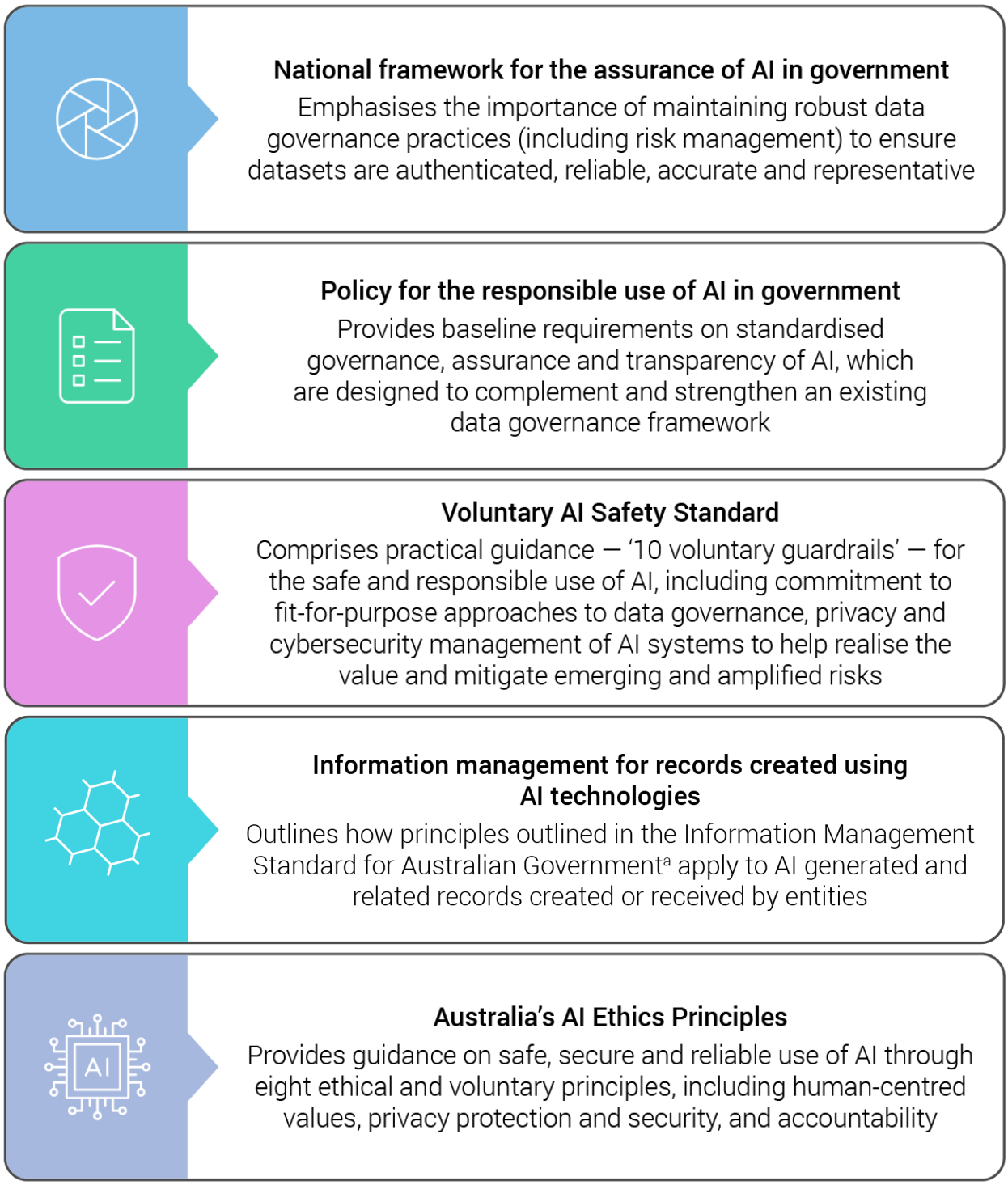
A data strategy is designed to provide a clear entity-wide approach to managing, governing and leveraging data as a strategic asset. It is typically more specific than an information governance framework, setting out a detailed plan for capturing, managing, using, storing and protecting data to achieve required objectives, improve decision-making and drive innovation. A data strategy should identify what data is required, what data will be collected, how the data will be used, risks to effective data management and measures of success.

For further guidance on establishing data governance and an enterprise-wide data strategy, entities can refer to the Office of the National Data Commissioner's Foundational Four.

AI should be integrated into an entity's information governance framework and data strategy to ensure that AI-driven decisions, models, and technologies are used responsibly, securely, and in alignment with business objectives. Entities that use or are planning to use AI in their business should:

- specifically address the management of data used for AI in their information governance framework, including monitoring and validation of data that will be input into and generated by an AI technology;
- regularly review their information governance framework and monitor risks on an ongoing basis because of the evolving nature of AI; and
- ensure that they meet the requirements of the Policy for the responsible use of AI in government (provided that they are not exempted from applying the policy).

Key resources on integrating AI use into data governance



Note a: Information Management Standard for Australian Government.

Case study 3. Governance of AI data at the ATO

In 2024–25, the ANAO examined AI governance arrangements in the Australian Taxation Office (ATO). The ATO used AI to analyse data for assessing non-compliance risks, drafting communications, and developing visualisations.

Within the Australian Government sector, requirements and guidance for AI governance and management were evolving at the time of the audit. The ATO was adapting existing data management and data governance arrangements and introducing new arrangements to support its adoption of AI, including to support risk management and assessments of ethical considerations. The audit highlighted the following.

- The ATO was using its existing data governance arrangements for AI, but had identified that its use of AI needed additional governance to account for AI-specific risks.
- The ATO did not have a comprehensive register of its AI. A comprehensive register could include information about the data used in both the training and operation of AI.
- The ATO had data-related enterprise risks. These risks were about maximising the value of data and analytics while also managing the misuse of data and analytics. Both risks were 'above tolerance' at the time of the audit and the ANAO found that oversight, including monitoring and review, of these risks should be enhanced.
  - The ATO had data ethics principles that aligned with Australia's AI Ethics Principles. It had developed arrangements aimed at embedding these principles into its use of data and analytics, including AI. However, required data ethics assessments were not always completed for AI models. The ANAO recommended that the ATO's data ethics framework be better integrated into existing processes, with monitoring, assurance and reporting arrangements over the implementation of the data ethics framework.

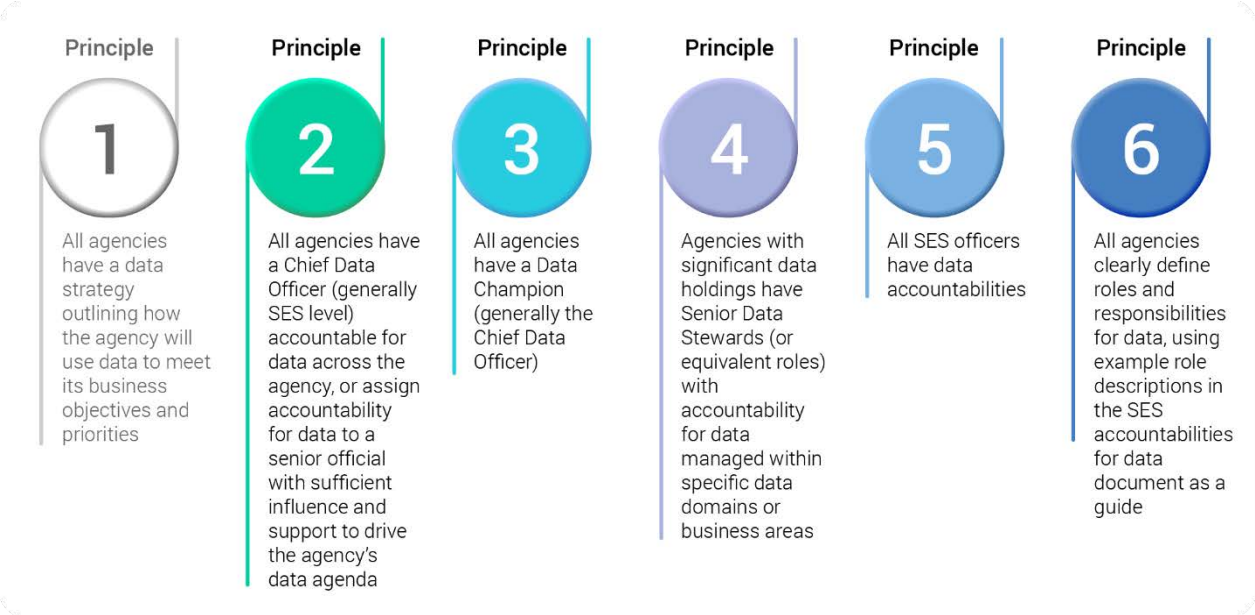
To read more, see Chapter 2 of Governance of Artificial Intelligence at the Australian Taxation Office.

Lesson 3: Establish data leadership and define roles and responsibilities

The governance and use of data should be the responsibility of a data lead (usually a Chief Data Officer or equivalent data leadership role). The data lead provides strategic oversight and ensures that the entity meets government expectations for data management. Clear roles and lines of responsibilities under the data lead supports entities in timely and appropriate data decision making.

Five of the six principles outlined in the Department of Finance's SES Accountabilities for Data guidance refer to data roles and responsibilities.

Principles to strengthen SES accountabilities for data



By following the six principles, entities can increase and maintain consistency of data governance practices and quality within the organisation as well as across the APS. A Chief Data Officer or equivalent is typically accountable for enterprise-wide governance and use of data as a valuable and well-governed asset across the entity, and building entity data capabilities (see also the Chief Data Officer Information Pack). SES staff more generally should be accountable for proper use of government data within their areas of business responsibility, in accordance with the entity's information governance framework, and for supporting efforts to build the entity's data capabilities.

To further support accountability and transparency of decision-making, the Chief Data Officer or equivalent should consider establishing a data team with defined member roles and responsibilities, such as:

- a data champion — promotes best practice use, sharing and re-use of data throughout the organisation and across the APS;
- data custodians — responsible for the integrity, availability and use of specific data assets;
- senior data stewards — responsible for daily management of specific data assets, including quality and access; and
- data analysts — responsible for ensuring that they access and use data appropriately.

Case study 4. Defining the role of Chief Data Officer

The Department of Social Services' (DSS) annual performance statements were audited as part of the ANAO's 2023–24 performance statements audit program.

- ✓ DSS defined the role of its Chief Data Officer with specific responsibilities outlined for annual performance statements reporting and performance reporting communities of practice (groups of individuals who engage in collective learning to improve work practices).

The ANAO observed that a Chief Data Officer can:

- help entities build robust, data-driven performance reporting frameworks; and
- establish clear lines of responsibility for data quality and appropriateness by allocating data owners for performance measures.

To read more, see paragraph 3.29 and Appendix 1 of Performance Statements Auditing in the Commonwealth — Outcomes from the 2023–24 Audit Program.

Lesson 4: Document data methodology with data processes mapped end-to-end

Greater accountability, transparency and oversight of individual data processes is achievable through clear methodology documentation for data handling. Clear documentation of data methodology supports entities in understanding, replicating and confirming the accuracy and completeness of that data. End-to-end data process mapping explains how data flows across systems and teams, highlighting dependencies, risks and opportunities for improvement. This makes data practices more resilient and contributes to assurance that business outcomes are underpinned by quality data.

Entities can realise the benefits of good data governance by requiring clear documentation that specifies:

- data ownership and stewardship — information on individual and team roles and responsibilities for specific datasets and processes;
- data classification and categorisation — define the different types of data and how it is classified to make it discoverable and useful;
- data sources and systems — reliable and verifiable data sources and data systems;
- end-to-end processes — mapping the flow of data from start to finish ensures that data remains consistent and accurate across platforms and systems and enables data teams to promptly locate required data at any point in time and assist stakeholders in tracking progress toward achievement of business objectives;
- data lifecycle management — data processes and standards for data collection, retention and disposal. Entities may refer to the Data Maturity Assessment Tool or the Data Lifecycle View outlined in the APS Data Capability Framework to identify areas for improvement to their data lifecycle management practices;
- quality standards and assurance processes — confirm that underlying data is relevant, complete and accurate; and
- auditing and monitoring practices — data can be formatted and organised to enable audit and assurance of that data, and to support change management procedures (such as changes to data access and modifications to data).

Data documentation should be clear and sufficiently detailed to support business continuity, mitigating risks such as loss of knowledge through staffing or machinery of government changes.

Where entities need to work together with data to achieve a common purpose, data documentation helps entities collaborate effectively.

Case study 5. Mapping data processes to calculate performance measure results

During the 2023–24 audit of Services Australia's annual performance statements, the ANAO observed that:

- ✓ Services Australia had developed process maps that outlined end-to-end data processes to calculate reported results for each performance measure. These process maps assisted in developing line areas' understanding of their roles and responsibilities in producing results for each performance measure.

To read more, see Appendix 1 of Performance Statements Auditing in the Commonwealth — Outcomes from the 2023–24 Audit Program.

Case study 6. Cross-agency data management

The departments of Industry, Science, Energy and Resources, Social Services, and Finance and the Digital Transformation Agency worked together on the Streamlining Government Grants Administration (SGGA) Program. The program was to deliver simpler, more consistent and efficient grants administration across government. One of the four core deliverables of the program was to establish a data warehouse to improve cross agency reporting and analysis of grants data.

- × The core functionality of the data warehouse was not delivered due to a lack of interface between different systems, and variations in data and formats.
- × Data was incomplete and inadequate, which:
  - affected the accuracy and currency of reporting;
  - meant that recipients could be double funded due to gaps in common source data; and
  - resulted in data not being used to better manage and target grants funding.

Establishment of the intended data warehouse was considered not achieved.

To read more, see paragraphs 2.61–2.66 of Operation of Grants Hubs.

Lesson 5: Strengthen assurance over third-party data

Strengthening assurance over third-party data is crucial for maintaining data integrity, privacy, and compliance. Entities that outsource data collection or analysis should establish processes with firm controls to obtain assurance over the quality of the data and how results have been calculated. Essentially, entities should ensure that third-party data, data analysis and reporting are reliable and verifiable.

The services of third-party data providers may be sought to address business needs, such as managing internal resource constraints and capability gaps. For example, an entity with limited resources may not be able to collect and analyse large amounts of data within a short timeframe.

It may opt to use and analyse data collected by others, or outsource data collection and analysis to a third-party provider.

Outsourcing may introduce heightened risks, for example, to data integrity, security, privacy and regulatory non-compliance. Data risks may be identified, mitigated and addressed by implementing controls as part of a broader risk management strategy. Controls should be fit for purpose, with reporting obligations usually specified as part of a formal arrangement, such as the entity's contract or grants management arrangements. Controls to ensure delivery of agreed programs and services include:

- conducting regular due diligence, such as provider risk assessments and audits to help ensure third parties adhere to required practices;
- integrating third-party data into existing data governance frameworks (e.g. validation checks, access controls and monitoring) to help reinforce trust and ensure that data remains fit for purpose throughout its lifecycle; and
- obtaining control reports on the effectiveness of third-party systems, including their reliability and data security measures.

IT security controls are a key issue, especially with regard to entities that outsource software, hardware or infrastructure services under a cloud computing arrangement (CCA). During 2023–24, 89 per cent of Australian Government entities that the ANAO audited used one or more CCAs. Under CCAs:

- third-party cloud providers may supply a Service Organisation Controls (SOC) certificate to confirm that IT security controls were designed, implemented and operating effectively; and
- entities retain accountability and responsibility for ensuring that contracted IT services meet legislative and policy requirements, including the Protective Security Policy Framework and the Australian Government Information Security Manual.

Accordingly, receipt and review of a SOC certificate provides assurance over the implementation, design and operating effectiveness of controls included in contracts, including data security, privacy, process integrity and availability. Contrary to this assurance process, the ANAO's 2023–24 financial statements audit work found that:

- 75 per cent of Australian Government entities did not receive a SOC certificate for all CCA services provided; and
- 82 per cent did not have a policy or procedure requiring formal review and consideration of a SOC certificate.

Case study 7. Third-party controls in Snowy Hydro

Snowy Hydro Limited (Snowy Hydro) generates energy to supply the National Electricity Market and provides energy as a retailer through the Red Energy and Lumo Energy brands.

- ✓ Snowy Hydro's financial management information system was provided under a cloud computing arrangement, with the provider supplying Snowy Hydro a Service

Organisation Controls report prepared by an independent auditor. The report identified weaknesses in the operating effectiveness of IT controls that impacted data security.

- × Snowy Hydro did not have a formal process for periodic review of Service Organisation Controls reports and did not address noted deficiencies.

To read more, see paragraphs 17, 2.57–2.66 and 4.3.81–4.3.83 of Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2024.

Questions for reflection

Lesson 1: Value data as an asset

Does our entity have a culture that values curiosity, evidence and learning from data?

- Does our entity have leadership commitment, including a sole authority (Chief Data Officer or equivalent data leadership role) responsible for all entity data and for fostering a culture that values data?
- Does our entity consider from the outset what data is required to achieve business objectives?
- Does our entity collect and use data with a purpose, such as for evidence-based policy, and to evaluate and measure performance?
- Does our entity select and design systems based on the required data outputs?
- Does our entity have clear methodology documentation (such as standard operating procedures and workflows) that enables users to easily locate required data at any point in a process?
- Does our entity have appropriate controls in place to assure the integrity of data, such as regular data checks and sign off by senior staff certifying data quality and integrity?
- Does our entity uplift staff data capability through learning?
- Does our entity regularly assess its data maturity, such as by using the Data Maturity Assessment Tool?

Lesson 2: Develop an information governance framework and data strategy

Does our entity have an information governance framework and a data strategy?

- Does our entity's information governance framework provide broad oversight of our organisation's data assets and data management approach to achieve business goals?
- Does our entity's information governance framework set out
  - drivers for data, such as legislation, risk and business needs?
  - the environment within which data is created and/or captured, collected and managed?
  - the principles that guide data design, capture, management and use?
  - roles and responsibilities, including leadership, as they relate to data?
  - consistent understanding and use of data across systems within the organisation and with other entities?
  - controls to protect against risks to data and to preserve the integrity of data?

  - how ethical considerations are embedded into data and AI policies?
  - senior management commitment to uphold data governance?
- What actions does our entity take to embed information governance into its culture, such as training and guidance for staff?
- Does our entity's data strategy align with our organisation's information governance framework, with greater detail on the approach to data creation, capture, collection, management and use of data?
- Has our entity considered the Office of the National Data Commissioner's Foundational Four in establishing data governance and an enterprise-wide data strategy?
- Has our entity integrated AI into our information governance framework and data strategy to ensure responsible and secure AI use and alignment with business objectives?
- Does our entity regularly review and evolve our information and data framework and strategy?
- If applicable, does our entity meet the requirements of the Policy for the responsible use of AI in government?

Lesson 3: Establish data leadership and define roles and responsibilities

Does our entity have an established data leader and defined data team roles and responsibilities?

- Does our entity refer to the SES Accountabilities for Data guidance to establish data roles and responsibilities?
- Does our entity have a Chief Data Officer or equivalent who is accountable for enterprise-wide governance and use of data as an asset within the entity, and building entity data capabilities?
- Does the role of our entity's Chief Data Officer or equivalent align with the Chief Data Officer Information Pack?
- Does our entity hold SES staff accountable for the proper use of government data within their areas of business responsibility?
- Does our entity clearly document data roles and responsibilities?

Lesson 4: Document data methodology with data processes mapped end-to-end

Does our entity document data methodology with processes mapped end-to-end?

- Does our entity classify and categorise data to make it more discoverable and useful?
- Does our entity document data sources and systems?
- Does our entity document end-to-end processes?

- Does our entity manage entire data lifecycles (using the Data Maturity Assessment Tool or the Data Lifecycle View outlined in the APS Data Capability Framework)?
- Does our entity implement quality standards and assurance processes?
- Does our entity implement auditing and monitoring practices?
- Is our entity's documentation clear and sufficiently detailed to support business continuity and mitigate risks such as loss of knowledge through staffing changes?

Lesson 5: Strengthen assurance over third-party data

Does our entity have strong assurance over any third-party data?

- Does our entity clearly understand how third parties collect data?
- Does our entity have assurance over the quality and integrity of third-party data?
- Does our entity implement appropriate controls to identify, mitigate and address data risks?
- Does our entity integrate data reporting obligations as part of formal arrangements, such as contracts or grants management agreements?
- Does our entity conduct regular due diligence, such as provider risk assessments and audits?
- Does our entity integrate third-party data into existing data governance frameworks (e.g. through validation checks, access controls and monitoring)?
- Does our entity obtain control reports on the effectiveness of third-party systems, including their reliability and data security measures?

Further reading

ANAO links

2023–24 Major Projects Report | Australian National Audit Office (ANAO)

Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2024 | Australian National Audit Office (ANAO)

Governance of Artificial Intelligence at the Australian Taxation Office | Australian National Audit Office (ANAO)

Performance Audit Process | Australian National Audit Office (ANAO)

Performance Statements Auditing in the Commonwealth — Outcomes from the 2023–24 Audit Program | Australian National Audit Office (ANAO)

Reporting Meaningful Performance Information | Australian National Audit Office (ANAO)

External links

Key legislation and policy

Privacy Act 1988 - Federal Register of Legislation

Data Availability and Transparency Act 2022 - Federal Register of Legislation

Freedom of Information Act 1982

Protective Security Policy Framework

Other

AI in government policy | digital.gov.au

APS Data Capability Framework | Australian Public Service Commission

Building trust in the public record | naa.gov.au

Chief Data Officer Information Pack | Department of Finance

Data and Digital Government Strategy

Data Ethics Framework | Department of Finance

Data governance and management | naa.gov.au

Data Maturity Assessment Tool | Department of Finance

Framework for the Governance of Indigenous Data | aga

Foundational Four | Office of the National Data Commissioner

Information management | Department of Finance

Information management for records created using Artificial Intelligence (AI) technologies | naa.gov.au

Information management legislation | naa.gov.au

Information Management Standard for Australian Government | naa.gov.au

National framework for the assurance of artificial intelligence in government | Department of Finance

SES Accountabilities for Data | Department of Finance

Voluntary AI Safety Standard | Department of Industry Science and Resources