Australian Government
Department of Finance

Australian Government Data Governance Framework

September 2025

Contents

Australian Government 1

Data Governance Framework 1

1. Introduction 4

2. Purpose 4

3. Context 5

3.1 What is data governance? 5

3.2 Why is data governance important? 7

3.3 Approach to data governance 7

4. Key aspects of data governance 9

4.1 Strategy and planning 9

4.2 Data privacy and safeguarding 10

4.3 Organisational structures 11

4.4 Leadership 12

4.5 Culture 13

4.6 Technology 14

4.7 Data utilisation 15

5. Actions to achieve good data governance 17

6. Conclusion 17

Acknowledgements 18

Bibliography 18

Attachments 18

Attachment A – Australian Government Data Governance Checklist 19

Attachment B – Examples of Data Lifecycles 22

Attachment C – Data Governance Resources 25

© Commonwealth of Australia 2025



This work is licensed under a Creative Commons Attribution 4.0 International CC BY 4.0 licence with the exception of the Commonwealth Coat of Arms and the Department of Finance logo. Attribution for this work should be listed as Australian Government Data Governance Framework, Department of Finance 2025.

1. Introduction

Effective data governance enables public sector officials to treat data as a strategic asset. It ensures that data is accurate, accessible, secure and responsibly managed to support better policy making, service delivery, regulatory oversight and public trust.

As government officials, most of us are defining, producing and/or using data as part of our everyday jobs. Data is crucial in our roles and all Australian Government agencies have data related responsibilities under the Data and Digital Government Strategy, the *Data Availability and Transparency Act 2022*, the Framework for Governance of Indigenous Data, and a range of other government initiatives, frameworks and legislation.

For agencies and APS Officers, it is important to know what data you have, the condition it is in, how it was collected and what it can be used for. We know from the APS data maturity assessment process (first held in 2024) that many agencies are struggling with the basics of data governance. This framework aims to help you and your agency be confident in how data is used and understood in your agency.

2. Purpose

This framework is a general resource for all Australian government officers, both with and without direct data responsibilities, to build data maturity through a common understanding of data governance across the APS. For officers in data roles, such as Chief Data Officers (CDOs), data custodians and data users, it provides guidance on how your agency can –

- tailor its governance approach
- align practices with whole-of-government data policies and principles
- define clear role and responsibilities for managing data assets
- improve data quality, sharing, interoperability, and lifecycle management
- support compliance with legal frameworks, and
- facilitate safe, consistent and efficient reuse of data across agencies

This framework summarises guidance from key Australian government data governance documents and collates examples of good data governance practices for you to explore.

The framework also includes a checklist of governance practices if you need guidance or for comparison. This framework provides the basics of data governance your agency can adapt to suit your needs.

Want to skip to the specifics of data governance straight away?

Please skip ahead to the “Achieving good data governance” section of this framework and also the resources at Attachments A, B and C. Attachment A is a handy checklist of questions you may want to consider.

3. Context

3.1 What is data governance?

Put simply, data governance is the documented structures and activities in your agency that provide confidence and control in managing the data created in your agency's systems and processes, as well as the insights that come from the data, over the life of the data.

Depending on your agency's data activities and responsibilities, your agency's data governance approach could be documented in a detailed data governance strategy, or something simpler like a data governance statement. It could be a standalone document or within another corporate document. Your process in developing your data governance approach will document your research of good data governance practices and the decision-making process to identify what suits your agency's context.

Data governance sits alongside digital and ICT data management and records management (or information governance) by focussing on the way an entity adds value to data by transforming it into knowledge and insights. Data governance helps embed the vision outlined in the agency's Data Strategy. Importantly, it formalises accountability both for data and its impact for the agency.

Similarly to these other forms of management, data governance is documenting and enacting –

- the agency's vision for data governance
- clear leadership, roles and responsibilities
- processes for oversight and reporting
- standard procedures for both business-as-usual and to respond to incidents, and
- regular procedures for evaluation, review and continuous improvement.

In this framework, we use the same definition of data as the *Data Availability and Transparency Act 2022* - data is any information in a form capable of being communicated, analysed or processed (whether by an individual or by computer or other automated means). Data gains in value when collated, organised and evaluated, and transformed into knowledge or insights.

In addition, an agency's data strategy may provide further detail and advice on how data is defined within their own context, in a way that is useful for their business.

Agencies (or their authorised Agents) collect the data produced by their systems and processes, so they can analyse it and interpret it into meaningful insights.

Which insights are meaningful, and the form those insights take, are very much dependent on the audience. At the very basic level, data helps us understand who is interacting with a system or process, what they are doing and when they are doing it. From this, we can find out who may be missing out, how it could be made better for users or if it is achieving good outcomes.

A note on data, information, ICT and records management

Data is held in ICT systems that manage the practical aspects of collection, storing, moving, decommissioning and safeguarding data. Data management from an ICT perspective is focussed on execution of processes. While it supports the analysis that produce insights, ICT areas are generally not responsible for undertaking analysis or deciding which insights will be valuable for the agency.

Entities also produce a significant amount of information. Information is data that has been transformed for a particular purpose – the practical result of the insights gained. Information can be forms that cannot be readily analysed, such as audio, visual or artistic formats. It includes the day-to-day administrative records and documents produced as part of an entity's functions. Managing, recording and safeguarding this information typically occurs though records management and archiving which are critical for preserving corporate and government history.

Data and datasets held in your agency's business system, like other information created and received in relation to Australian Government business, are Commonwealth records and must be managed in accordance with the *Archives Act 1983*. Other legislation your agency should be aware of regarding managing their information includes the *Privacy Act 1988* and the *Freedom of Information Act 1982*.

The Data Maturity Assessment Tool Guide has the following advice about data and information - *Data is a collection of discrete or continuous values that convey information. Data differs from 'information', in that data is the raw material of information, while information is data in context. For instance, a sales report from the last quarter is information, whereas the numbers from the warehouse which informed the sales report is data.*

An agency should have a holistic approach to data and information governance at the organisation level. However, there is flexibility on processes and approaches to these depending on the agency's needs and responsibilities for data.

Sources: Data Availability and Transparency Act 2022 - Federal Register of Legislation; Data Maturity Assessment Tool Guide; National Archives of Australia 'Data governance and management'; National Archives of Australia 'Retaining, managing and disposing of data and datasets'; ONDC (see 'Definitions Guide'); DISR Data Strategy 2021-2024; Archives Act 1983; Privacy Act 1988; and Freedom of Information Act 1982. For a more comprehensive list, please refer to Attachment C: Resources.

3.2 Why is data governance important?

Having governance for your data is no different to having governance for your agency's finances, performance and property. Data is a valuable agency asset, and its risks need to be managed accordingly.

Data governance allows you to –

- realise greater value and benefits from data through more effective utilisation and understanding across the agency
- understand your agency's impact, and to deliver better programs, services and outcomes for users and stakeholders
- enable evidenced-based decision-making and enhanced policy development
- more easily meet commitments to reporting, such as Closing the Gap
- manage data more effectively across its lifecycle, ensuring its discoverability, accessibility, quality and security
- ensure your agency's data processes are prepared for use by emerging technologies such as AI
- respond quickly and adequately when there are issues with your data as you have a strong understanding of, and have documented, your data ecosystem
- use data strategically
- improve data maturity
- take proactive steps to reduce the risk of data mishandling and avoid data breaches and malicious activity
- enable the agency to quickly and confidently address queries about the way it handles data, and provide documented evidence on how it does so and the rationale for its practices for example Inquiries, audits and FOI, and
- ensure your agency is meeting its obligations around record keeping and management.

Sources: Data Maturity Assessment Tool; *Freedom of Information Act 1982*; and SES Accountabilities for Data

3.3 Approach to data governance

It is important to understand your agency and its needs around data to tailor your data governance arrangements. You may want to consider agency attributes and factors such as –

- agency size and resourcing
- agency type
- data type and sensitivity
- data production levels and sources
- data workload
- data reporting frequency
- criticality of data-related output and functions
- agency goals and aspirations
- spread of data across your agency, and
- the existing data culture and attitudes to data.

It is also important that your agency invests time to understand –

What –

- are its wider responsibilities, goals and aspirations
- it wants and needs to achieve with data
- its data responsibilities are
- its data ecosystem and processes end-to-end
- stories or messages it wants to communicate that can be supported by data
- legislation, regulation, policies or other commitments is your agency bound by

How –

- data can and should support its goals and priorities

Why –

- data matters to its operations and functions
- it wants to improve data governance

When –

- key events happen across the data lifecycle for your agency (e.g. data collection and reporting)
- are the critical dates for data-related actions, to ensure your agency and stakeholders have the data they need to meet their commitments

Once your agency invests time in understanding its data holdings, aspirations and goals, and the risks and opportunities around these, it can –

- look at which of the key aspects of data governance to implement and,
- who should hold the various roles and responsibilities.

You may find that your agency's data strategy covers much of this context, and you can use that as the basis for developing your data governance approach.

4. Key aspects of data governance

This section introduces what data governance can achieve for your agency and key aspects involved in data governance.

4.1 Strategy and planning

Your agency's approach to data governance should align with other corporate strategies and policies, such as the Corporate Plan, Enterprise Risk Management Policy and ICT or Digital Management Frameworks. In particular, data governance must have a strong connection with your agency's Data Strategy.

All agencies must have a Data Strategy, to meet commitments made in the whole-of-government Data and Digital Government Strategy. A data strategy prescribes your agency's approach to managing, governing and leveraging data as a strategic asset.

A data strategy will outline the agency's vision and priorities for collecting, storing, sharing and using data to achieve agency strategic objectives.

Depending on your agency's data holdings, aspirations and goals, your data strategy can be comprehensive or brief.

Your agency should take into account whole-of-government obligations such as under the Data and Digital Government Strategy, the *Data Availability and Transparency Act 2022*, the Framework for Governance of Indigenous Data (please also see Attachment C).

A note on data governance and data risk management

As with data governance, your agency's approach to data risk will depend on the nature of its data activities and data holdings.

As data risk management can be extremely complex and technical, this Framework is limiting its focus to the interaction between data governance and data risk.

Your data governance will refer to and support your agency's data risk approach in a way that suits your agency.

The data risk approach may be within the data governance document, or be a separate detailed document. It may be a part of cyber, ICT or digital risk approaches, or policies around privacy and responses to data breaches. Areas within an agency with particular data responsibilities, or sensitive data assets, may need additional risk approaches.

At a minimum, your agency should have a documented approach to risks around the aspects of data not covered elsewhere (such in digital systems or privacy risk management). The approach should cover the aspects of transforming data into insights, and the use of those insights, if these are applicable to your agency. Your data risk approach should be developed with feedback from people in key responsible roles and subject-matter-experts for data, digital and privacy in your agency.

We have included some resources on data risk as a starting point.

Sources:
Data Strategies - DISR Data Strategy 2021- 2024; AIHW Strategic directions 2022–2026;
Data Risk - Risk | User Guide | Data.gov.au; Data Maturity Assessment Tool; Five Safes framework | Australian Bureau of Statistics; Records, information and data risks | NSW Government; Data and Digital Government Strategy; Framework for Governance of Indigenous Data.

4.2 Data privacy and safeguarding

Data privacy is protecting information about who people are, what they do and what they believe – in other words, personal information. Other types of data that need protection include data about sensitive environmental or cultural sites and information that could have a commercial or national security impact. Safeguarding data at all stages of its lifecycle protects people from harm caused by issues such as data misuse and privacy breaches. It also helps maintain public trust of government handling and use of data.

Your agency must ensure compliance with the data legislation, regulations and policies that apply to all Australian Government agencies and to your own agency (or its data assets, functions or activities). Good data governance complements and supports your agency's efforts to meet its obligations for data and more broadly.

Examples include, but are not limited to – *the Privacy Act 1988 (Cth);* the Australian Privacy Principles; the Notifiable Data Breaches Scheme; Framework for the Governance of Indigenous Data; the Information Security Manual; Protective Security Policy Framework; National Statement on Ethical Conduct in Human Resources and; Data Ethics Framework.

Your agency may decide that additional measures are needed to ensure data privacy, such as a breach response plan, or co-design of data activities with key stakeholders.

All of these should be referenced in your data governance approach and should also align with ICT and physical security obligations.

Please refer to section 4.6 for further data privacy and safeguarding in relation to technology.

Sources: *Privacy Act 1988 (Cth);* Australian Privacy Principles; Notifiable Data Breaches Scheme; Framework for the Governance of Indigenous Data; Information Security Manual; Protective Security Policy Framework; National Statement on Ethical Conduct in Human Resources; Data Ethics Framework; and Australian Government Agencies Privacy Code.

4.3 Organisational structures

Ensuring appropriate organisational structures in your agency means data related decisions are made by the right people at the right level, and there is a clear organisational approach to managing data. It also means decisions are captured and can be tracked for insights, accountability and record-keeping.

Organisational structures include executive groups, specifically defined roles and responsibilities across the organisation as well as supporting activities such as communities of practice. Data governance groups can be embedded in your organisation as data governance is part of corporate considerations and functions. More detailed advice on setting up senior data governance groups in different types of agencies can be found in the SES Accountabilities for Data.

As a practical example, your agency could make governance a standing item at a regular SES-level corporate meeting. Alternatively, agencies may have a specific senior executives' group to discuss data, plus groups at other levels such as data analyst groups or a community of practice.

Your organisation should consider representation at whole-of-government data governance groups where appropriate, such as the Data Champions Network, Chief Data Officers Group, Deputy Secretaries Data Group and Secretaries Data and Digital Committee. There are also a number of data-related communities of practice and officer-level groups.

Regardless of whether your agency is hierarchical or flat, someone needs to be responsible and known for having authority over particular data sets and your agency's overall data. Staff with data responsibilities will need to work closely with their colleagues in the areas of Information Security, Records Management, Legals, Privacy and Digital/ICT management.

At a minimum, agencies should have the following four key data roles –

Chief Data Officer (CDO) – an essential role that ***cannot be delegated***. The CDO is a SES-level officer, with overarching responsibility and accountability for data across your agency. The Australian Government Data and Digital Government Strategy commits agencies to appoint CDOs to manage data within their agencies.

The following roles can be delegated, or can be part of the CDO role –

- **Indigenous data champion** – a senior level person responsible for guidance and support in the governance and management of Indigenous data assets. The Framework of Governance of Indigenous Data commits agencies to appointing an Indigenous data champion.
- **Data champion** – promotes best practice use, sharing and re-use of data within their agency and across the APS.
- **Responsible officer** – a person at an appropriate level who has direct day-to-day authority over specific data assets and is usually the key contact for the data asset.

The key here is the roles, and their responsibilities. There is flexibility for agencies to use whichever naming they prefer for their internal role titles, and also where the roles lie in their agency.

In a smaller agency, a single person might have responsibility for multiple roles; for example, your indigenous data champion could also be your CDO. The APSC Data Professions website has useful guidance on building data capability, including the data leadership skills and capabilities outlined in this Framework.

Sources and for a more detailed list of data roles and responsibilities: APS Data Capability Framework; SES Accountabilities for Data; Framework for Governance of Indigenous Data; CDO information pack; and APSC data profession website.

4.4 Leadership

Aside from the specific roles mentioned above, all SES play an important role in data governance leadership.

Leadership involves championing effective information and data management across your organisation, promoting good information and data management practices.

Practical examples of leadership in your organisation may include –

- embedding data in corporate and strategic considerations
- ensuring officers under their management are aware of their responsibility for managing and monitoring data throughout its lifecycle
- supporting and fostering a culture of good data management (see culture and technology section)
- providing guidance to their staff members on managing sensitive data
- ensuring staff have adequate time to undertake their data responsibilities.

SES in your agencies should familiarise themselves with and apply the principles and accountabilities in the SES accountabilities document and the Chief Data Officer information pack in their day-to-day work.

Ideally, SES leadership in your agencies should be responsible and accountable for encouraging, overseeing, and improving the use of data in decision-making in your organisation. Data governance groups should be embedded in executive decision-making structures.

More broadly, data leadership should be seen at every level so all staff members can appreciate and value data when creating or handling data.

Sources: SES Accountabilities for Data; CDO information pack and; Data Maturity Assessment Tool.

4.5 Culture

Ensuring your agency's people and systems effectively support your agency's data vision is an important step.

All APS officers contribute to and utilise their agency's data and insights. Influencing the culture of your agency so that everyone is acknowledged as 'data person' involves a supportive and authorising environment where staff have the ability and resources to make data-informed decisions. Seeking support from leaders can be an effective way to communicate and build confidence in utilising data internally and externally in your agency.

Trust must be built into your agency's culture by being transparent about its governance of data. Being transparent builds trust in government data more broadly and confidence that it is being accessed and used appropriately.

Depending on your agency's resourcing and needs, it may provide training, networking, employment or secondment and educational opportunities to attract the right staff and develop technical data skills to support staff to make data decisions.

Good data governance culture includes ensuring your agency's leadership and staff understand their role in fostering a culture where data assets are valued.

The APS Data Capability framework describes the capabilities for valuing data at a foundational level as follows –

- is familiar with organisational data assets relevant to their work.
- understands how those assets contribute value to the organisation.
- actively looks for opportunities to use data to support decision making, advice and research.
- uses insights from data to make informed decisions.

Agencies that value data as an asset would be better positioned to make evidence-based decisions and realise the economic, social, environmental and other benefits of good data.

Sources: Data and Digital Government Strategy; Australian Government Data Catalogue; QLD Data Governance; ANAO Insights: Audit Lessons – Governance of Data; and APS Data Capability Framework.

4.6 Technology

Once your agency understands its data needs, goals and aspirations it can decide what level of investment in technology is needed or if any specialist ICT infrastructure is needed at all. In the context of data governance, technology is leveraged to make data more discoverable, useable and manageable.

Utilising processes, tools, and technologies in new ways to enhance your data can lead to administrative efficiencies and support better decision making through better analytic insights. Current examples include Artificial Intelligence, Generative AI, Data Matching, Large Language Models and Machine Learning, noting the rapid evolution in this area makes future directions hard to predict.

The benefits from any analytic technologies are highly dependent on the quality of data they rely on. Data governance helps you understand whether particular emerging technologies are a worthwhile investment, based on your organisation's needs and the data quality required to utilise the technology safely. This helps your agency make considered choices about what is appropriate for you. You should monitor and evaluate its use, decide its effectiveness and where its focus should be in your organisation. Your agency is responsible for protecting individuals' privacy and managing risks. You should keep up to date with the progression of technological change and refer to the latest government advice and best practice.

Not every agency needs a specific focus on data innovation. For example, if they have limited use of data internally and externally, are new to data governance, or have limited resources.

Your agency must ensure they are using emerging technologies safely and responsibly following the latest government guidance which currently includes Australia's AI Ethics Principles, Data Ethics Framework, and the National framework for the assurance of artificial intelligence in government.

Sources: AI in government policy | digital.gov.au; Information security manual | Cyber.gov.au; Australia's AI Ethics Principles; National framework for the assurance of artificial intelligence in government; Policy for the responsible use of AI in government; Australian Responsible AI Index 2024; Data Ethics Framework; Voluntary AI Safety Standard; ISO/IEC 42001:2023 - AI management systems.

4.7 Data utilisation

Data is valuable when it is utilised for service delivery, analysis, publication or sharing to contribute to wider understanding of government activities across the APS. Good data management practices are essential to your agency understanding, describing and utilising your data throughout its lifecycle and (where needed and possible) preparing for your data to be shared outside your agency. You should consider the ONDC's data sharing principles in data sharing decision making. Making your data more reliable, relevant and easy to find and understand contributes to more robust decision making in your agency and maximising the value of its data.

You should also consider your processes for preparing your data for utilisation such as data cleansing, data matching and putting data in a format suitable for analytics technologies. You should follow the latest government's guidance for these activities for example the OAIC's guidance on Government data matching.

An example of good data quality involves agencies having a data quality standard and being reactive to data quality issues. Ideally, data quality involves the agency proactively monitoring and addressing data quality issues.

The approach to data quality should be aligned to the use and criticality of the data. Data that supports activities with direct impacts on individuals, communities and businesses (such as audit, enforcement and compliance) must have a high level of accuracy and scrutiny. Your data governance should include appropriate levels of oversight and assurance.

Mapping your data assets from authority and collection, through to use, and all the way to destruction, as well as its legal authority and interactions with other data assets and systems, helps you understand your agency's data ecosystem. Going through data lifecycles[1] helps agencies understand what they do when data is created or collected, what the agency does with the data, and how to manage it at end of life. Agencies with significant data holdings may have a more complex data ecosystem with a number of lifecycles. Agencies should have a plan to review their data ecosystem to strengthen their data management practices.

Agencies should have a clear understanding of the authority that allows them to collect data, and any restrictions that may be part of that authority. The authority may come from legislation, legal agreements or contracts, or necessary for operating the agency, its programs or services. This authority should be easily accessible to staff using the data and should be referred to in decisions around use of data. Data activities should also comply with any legislation, rules or requirements for the agency itself (for example, the *Australian Bureau of Statistics Act 1975*; the *Australian Institute of Health and Welfare Act 1987*; the *Census and Statistics Act 1905*; the *Federal Court of Australia Act 1976*)

[1] There is no standard format for a data lifecycle. Different agencies may have their own version of a data lifecycle they follow. Generally, data lifecycle stages include: creation; collection; publication; uptake and usage; sharing; and ending (archiving, destruction, return).

The Australian Government Data and Digital Strategy requires all government entities to make non-sensitive data open access by default. It must also comply with relevant laws and appropriate privacy, security and ethical controls for sharing sensitive data.

For agencies that have data holdings either themselves or with third parties, your agency or the entity that holds the data should consider –

- having both and internal and a public-facing list of the key data assets that may be publicly identified
- a description of what those assets contain
- whether they are legally shareable and a contact for requesting access to data.

Where possible, data that is non-sensitive (or sensitive data that has been anonymised) should be publicly available.

Mapping and understanding your data can help you identify the data that would be most valuable to external users. It also helps embed processes to ensure that the open data is safe, accurate and timely. Making safe versions (e.g. appropriately anonymised or de-identified) of your agency's most requested data could help reduce your data request or Freedom of Information Request workload.

It is important for your agency to clearly document its data holdings. This documentation can cover the following –

- collecting metadata (information which describes your data) in line with the Australian Government Recordkeeping Metadata Standard
- ensuring the currency of your data is clear such as the timestamp, source and collection methodology and where possible, advise how frequently the dataset will be updated
- ensuring Indigenous data is appropriately accessible and findable and, where possible, publishing that data in line with the Framework for the Governance of Indigenous Data
- improving data cataloguing by making data easier to find and access on DataHub to help your staff use the right data for the right purpose.

Once agency held data assets are mapped, and you have understood your data lifecycle you may share this information outside your organisation if: there is a business need; it is legally possible; and it is safe and ethical. This is an important aspect of achieving the Australian Government's commitment to data transparency, open data and sharing by making sure others know what your agency holds. You may want to leverage the Australian Government Data Catalogue to promote discoverability of your agency's data.

Sources: Australian Government Data Catalogue | AGA; Data and Digital Government Strategy; Intergovernmental Agreement on Data Sharing | Department of Finance; Freedom of Information Act 1982; ONDC's data sharing principles; Australian Bureau of Statistics Act 1975; the Australian Institute of Health and Welfare Act 1987; the Census and Statistics Act 1905; the Federal Court of Australia Act 1976; Australian Government Recordkeeping Metadata Standard; Framework for the Governance of Indigenous Data; Guide on Metadata Attributes | Office of the National Data Commissioner; Mapping the ONDC and National Archives' metadata requirements | naa.gov.au; Data Discovery Resources | Office of the National Data Commissioner; ABS Metadata; Australian Government Recordkeeping Metadata Standard; DataHub; OAIC Government data matching; Guide to data analytics and the Australian Privacy Principles.

5. Actions to achieve good data governance

The key to good data governance is understanding the key aspects of data governance, understanding your agency and then tailoring your approach to data governance to suit.

An agency's Chief Data Officer has overall responsibility for their agency's data governance. They are critical to creating the authorising environment both for the team developing the data governance approach, and the implementation and embedding of data governance.

As with all corporate governance activities and policies you should evaluate your data governance practices regularly and ensure they are fit for purpose. Some practical steps for the team developing an agency data governance approach are –

- Map out your agency's data holdings, needs, goals and aspirations.
  - You may ask your agency's CDO for your agency's Data Maturity Assessment report to understand its strengths and weaknesses and where you might want to redirect your agency resources to improving.
- Look for your agency's corporate and data strategy to ensure alignment.
- Take a look at the resources attached to this Framework:
  - Attachment A – Data Governance Checklist
  - Attachment B – Examples of Data Lifecycles
  - Attachment C – Resources

This Framework can also be found on the Public Data Policy webpage on the Department of Finance website.

6. Conclusion

Data governance is essential as our roles become increasingly intertwined with data. This framework aims to be helpful and flexible to give your agency the confidence to tailor an approach to data governance that meets its needs.

This framework is a living document, managed by the Department of Finance and publicly available on the Department of Finance website. Finance will periodically review the framework and its associated resources and update them accordingly.

Questions? Please contact us on datapolicy2@finance.gov.au

Acknowledgements

The Department of Finance thanks and appreciates the important contributions of the Data Governance Framework Working Group in producing this Framework.

Bibliography

Seiner, RS. (2023). *Non-invasive data governance strikes again*, Technics Publications, Sedona, Arizona.

Attachments

Attachment A – Data Governance Checklist

Attachment B – Examples of Data Lifecycles

Attachment C – Data Governance Resources

Attachment A – Australian Government Data Governance Checklist

This checklist covers some basic aspects for a data governance strategy or statement.

In preparing our data governance strategy, we have –

- ☐ Ensured it aligns and feeds back into to the agency's Data Strategy, ICT (including AI/Cyber) Strategy and Corporate Plan, and sought advice from those areas
- ☐ Covered a range of data activities and sources, including –
  - corporate data (eg HR, financials)
  - data produced by our entity's activities (eg program or service delivery, surveys, linked data assets and analysis)
  - data activities that third parties undertake for our entity
  - data acquisition and provision, including by sharing
  - dissemination and communication of insights
- ☐ Explored and documented our data end-to-end (data lifecycle), both at an entity level and for key data assets
- ☐ Looked at our entity's Data Maturity Assessment results to identify strengths and weaknesses (in particular, Questions 1-14, 30-47)
- ☐ Documented the development of our data governance approach, including the decision-making process and rationale for what is contained in our data governance approach
- ☐ Sought feedback from staff across the spectrum of data activities and expertise
- ☐ Reviewed key resources on data governance, to identify what is appropriate for the agency (see below)

Our data governance strategy or statement –

- ☐ Has identified individuals in the following roles, at a minimum –
  - Chief Data Officer, including the following roles that can be delegated
    - Data Champion
    - Indigenous Data Champion
  - Person responsible for particular data assets (an individual may be responsible for multiple data assets)
- ☐ Documents the agency's key data management meetings and reporting lines
  - At a minimum, data governance should be a standing item at a regular SES-level corporate meeting
- ☐ Has identified all other data roles appropriate to the agency's data activities, as well the individuals fulfilling those roles (an individual may have multiple roles, if appropriate)
- ☐ Holds all SES staff accountable for proper use of government data within their areas of business responsibility and is clear that all staff have data responsibilities
- ☐ Has a process to review and evaluate the strategy or statement to ensure it remains relevant, appropriate and effective.
- ☐ Has identified how the agency participates in Australian Government Data Governance Groups

Our agency's data governance documents include –

- ☐ A structure or flow diagram showing the agency's data governance structures and reporting lines
- ☐ A list of the agency's key data assets, the authority for the data collection and the team to contact for any queries, issues or concerns
- ☐ A consistent and documented process for –
  - data acquisition
  - data sharing
  - public release of non-sensitive or anonymised data (open by default)
  - addressing data quality and governance issues (aside from breaches dealt with elsewhere)
  - data obligations as part of formal arrangements with third parties, such as contracts or grants management agreements
- ☐ Policy and guidance documents –
  - standard operating procedures
  - metadata standard / data dictionary
  - data quality standards and assurance processes
  - auditing and monitoring practices

Our agency supports data governance by –

- ☐ Communicating internally to –
  - promote Government and APS commitments to data
  - make clear the agency's expectations of all staff regarding data
  - make it easy for staff to access the entity's Data Strategy and data governance documents, as well as other data guidance and resources
- ☐ Including data considerations in its corporate plan, and working to align corporate, data and digital goals
- ☐ Ensuring that the people responsible for data are included in decision around ICT, AI and emerging technologies

Tailoring your data governance document

Your agency's data governance needs may be met by a detailed data governance strategy, or something simpler like a data governance statement. At a minimum, your agency should have a documented approach, whether it is in the form or a standalone document or within another corporate document.

Your agency's Data Strategy will go into detail about your agency's data goals and needs, as well as your agency's approach to data literacy and maturity.

Resources:

Australian National Audit Office (ANAO) paper Insight Lessons – Governance of Data (2025).

Chief Data Officer Information Pack

Data and Digital Government Strategy

Data Maturity Assessment Tool

Data Profession | Australian Public Service Commission

Information Management Strategy webpage

Office of the National Data Commissioner's Foundational Four guidance

SES Accountabilities for Data

Attachment B – Examples of Data Lifecycles

What is a data lifecycle?

A data lifecycle is a way of understanding the data and analytics that your agency produces, uses and relies on, and the various states that data passes through throughout its existence. From a data governance perspective, these are more comprehensive than an ICT data lifecycle which tend to have a more system or technical focus. The various data lifecycles in your agency form a data ecosystem.

A data life cycle can be described or visualised in many ways. It will reflect the simplicity or complexity the agency's data ecosystem. It can help identify gaps, efficiencies and value-add at each step, or even steps that may no longer be appropriate. For this reason, it is also known as a 'data value chain'.

A data lifecycle document can have different versions for different audiences. A high-level version may show the basic steps, with additional documents showing more detail. A data lifecycle may be developed for particular data assets, particularly if the data being collected is sensitive and/or critical to the operations of the agency or its stakeholders.

Even if your agency outsources most of its data collection and analytics, you will still need to have a sense of the process, where your agency fits in and where responsibilities lie internally for that outsourced arrangement. Your agency will also have internal business and corporate data, which also needs to be understood, governed and managed.

This fact sheet gives four different examples of how a data lifecycle can be documented.

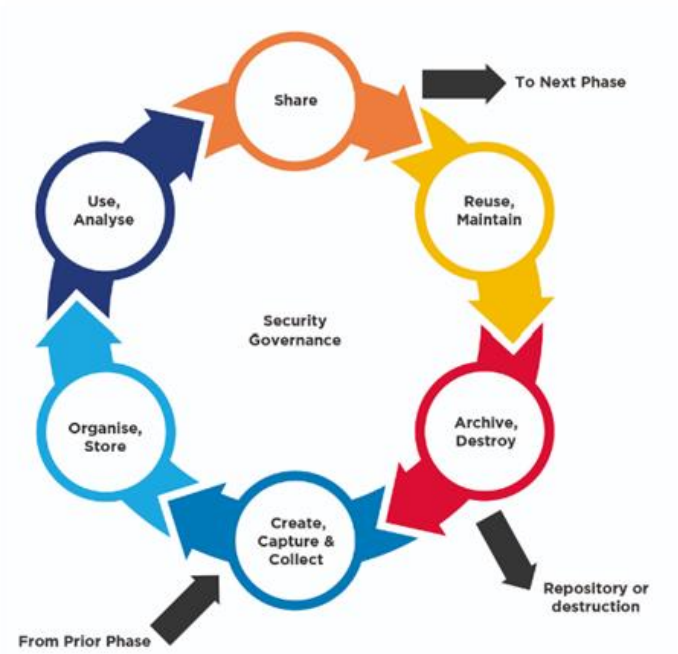
Example 1: Australian Government Data Capability Framework

Plan	The processes and resources are mapped out for the lifecycle of the data. The project's goals are stated, and a full data management plan is created.
Describe	The data is accurately described using the appropriate metadata standards.
Collect / Generate	Data is collected or generated by the individuals/organisation wanting to use it.
Store	The data is stored in a digital repository, is made secure and reusable. This often very quickly follows collection.
Prepare	The data is prepared, made ready for analysis and use.
Analyse / Use / Share	The data is analysed and used for the purpose for which it was collected or generated and reused for additional value.
Preserve / Destroy	Actions are taken to safeguard the long-term viability and availability of the data or destroy it if retention beyond a certain time is undesirable.

Source: APS Data Capability Framework | Australian Public Service Commission

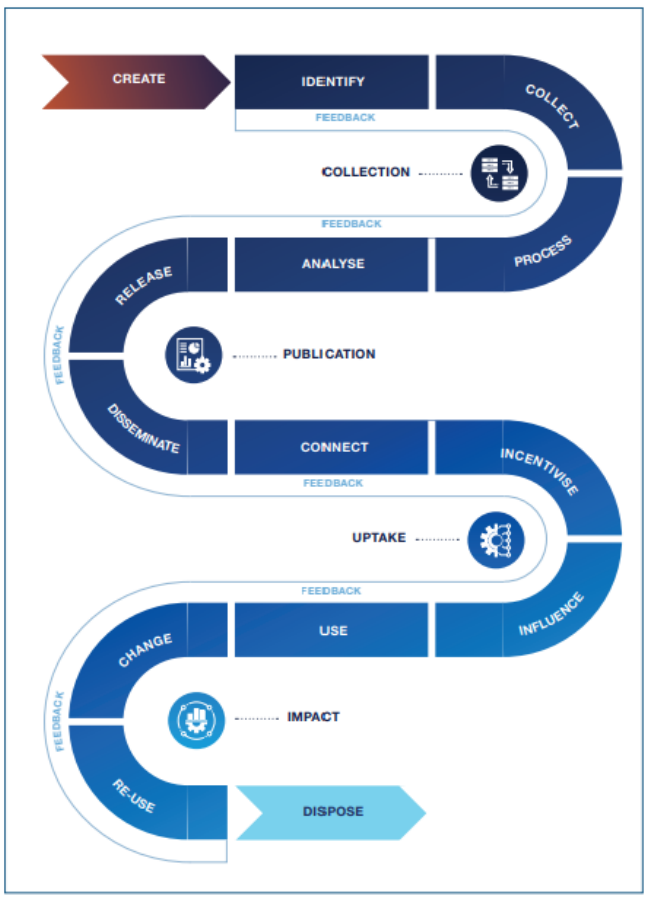
Example 2: NSW Government Infrastructure Data Management Framework – Data Management Lifecycle

Source: Data Management Life Cycle | Data.NSW



Example 3: Defence Data Strategy 2.0 - Decision Advantage in the Data Age – Data Value Chain

Source: Defence Data Strategy 2.0 - Decision Advantage in the Data Age | Defence



Example 4: AIHW Data Governance Framework 2022 (Public Edition)

Source: AIHW Data Governance Framework 2022

PART 6 – AIHW DATA POLICIES, GUIDELINES AND PROCEDURES

SECTION 49 - MANAGING THE DATA LIFE CYCLE

- *Collection establishment*
  - Proposals to establish a new collection
  - What constitutes an AIHW data collection?
  - Approval to establish a new collection
  - Data catalogue entry
  - Listing collections on the AIHW Web Site
  - Data Collection Management Principles
  - Quality Framework
- *Data acquisition*
  - Metadata
  - Data validation and data quality
  - Data storage and security
- *Data access and use within AIHW*
  - Access to AIHW ICT systems
  - Access to AIHW Research Only Network
  - Application of the separation principle
  - Data linkage
- *Data sharing and release for use outside the AIHW*
  - Data sharing and release
  - Preconditions for data sharing or release
  - De-identification
  - Approval for data sharing or release
  - Access arrangements for data sharing and release
  - The Five Safes framework
  - AIHW Data Governance Framework
  - Conditions for data sharing
  - Managing Statistical Outputs
  - Register of data shared or released
- *Data archiving, return, collection retirement and destruction*
  - AIHW data collections
  - Project specific data sets

Attachment C – Data Governance Resources

- Obligations, some examples include:
  - *Archives Act 1983;*
  - *Australian Bureau of Statistics Act 1975*
  - *Australian Institute of Health and Welfare Act 1987*
  - Australian Privacy Principles
  - *Census and Statistics Act 1905*
  - Data Availability and Transparency Act 2022 - Federal Register of Legislation
  - *Federal Court of Australia Act 1976*
  - *Freedom of Information Act 1982*
  - Notifiable Data Breaches Scheme
  - *Privacy Act 1988*
- Key Resources
  - ANAO Insights: Audit Lessons – Governance of Data.
  - APS Data Capability Framework
  - APS Data Professions website
  - Australian Government Data Catalogue
  - Data and Digital Government Strategy
  - Data Maturity Assessment Tool
  - Framework for Governance of Indigenous Data
  - Information Security Manual
  - Protective Security Policy Framework
  - SES Accountabilities for Data
- General Resources
  - ABS Metadata
  - ACSC/Cyber Incident Review Board - Australian Cyber Security Centre
  - AI in government policy | digital.gov.au
  - AIHW Strategic directions 2022–2026
  - Australia's AI Ethics Principles
  - Australian Government Agencies Privacy Code
  - Australian Government Recordkeeping Metadata Standard
  - Australian Responsible AI Index 2024
  - CDO information pack
  - Cross-Border Data Flows: Taking stock of key policies and initiatives' report - Organisation for Economic Co-operation and Development
  - Data Discovery Resources | Office of the National Data Commissioner
  - Data Ethics Framework
  - Data governance guideline | For government | Queensland Government
  - Data Governance Toolkit | Data.NSW
  - Data Interoperability Maturity Model
  - Data policies and standards | vic.gov.au
  - DataHub
  - Digital Trade Strategy - Department of Foreign Affairs and Trade
  - Discover and access Victorian Government open data | data.vic.gov.au
  - DISR Data Strategy 2021- 2024
  - Five Safes framework | Australian Bureau of Statistics
  - GSQ Open Data Portal | Business Queensland
  - Guide on Metadata Attributes | Office of the National Data Commissioner

- Home | Data.NSW
- Hosting Certification Framework (HCF) - Department of Home Affairs
- Information Management Strategy webpage
- Intergovernmental Agreement on Data Sharing | Department of Finance
- ISO/IEC 42001:2023 - AI management systems
- Mapping the ONDC and National Archives' metadata requirements | naa.gov.au
- NAA's 2024 Check-up Survey
- National Archives of Australia 'Data governance and management'
- National Archives of Australia 'Retaining, managing and disposing of data and datasets'
- National framework for the assurance of artificial intelligence in government
- National Statement on Ethical Conduct in Human Resources
- NSW Data Governance Toolkit
- OAIC Government data matching
- OAIC Guide to data analytics and the Australian Privacy Principles
- ONDC (see 'Definitions Guide')
- ONDC's Foundational Four guidance
- ONDC's DATA Scheme user accreditation
- ONDC's data sharing principles
- Open Data | Queensland Government
- Open Data Institute Guide to data practices
- Policy for the responsible use of AI in government
- QLD Data Governance
- Records, information and data risks | NSW Government
- Risk | User Guide | Data.gov.au
- Secure-by-Design Foundations includes secure-by-default. - Australian Signals Directorate
- Security of Critical Infrastructure Act 2018 (SOCI) - Department of Home Affairs
- The Data Governance Institute
- Voluntary AI Safety Standard
- Industry data classification framework - Department of Home Affairs