ACT Government

Data Governance and Management Guide

August 2020

NOTE: This ACT *Data Governance and Management Framework* was endorsed by Strategic Board on 5 August 2020

The Framework and support Guide will be designed for publishing at a later date.

For more, please contact the ACT Data Analytics Centre within the Office of the Chief Digital Officer – datalake@act.gov.au

ACKNOWLEDGEMENT OF COUNTRY

The Australian Capital Territory is Ngunnawal Country. The ACT Government acknowledges the Ngunnawal people as the traditional custodians of the Canberra region. The region was also an important meeting place and significant to other Aboriginal groups. The ACT Government acknowledges the historical dispossession and its continuing legacy for Aboriginal and Torres Strait Islander peoples and acknowledges their vital ongoing contribution to the ACT community.

Contents

INTRODUCTION

The ACT Government uses data every day to deliver essential and reliable services to the ACT community. We use data to inform our decisions when developing and delivering policies, programs and services. By investing in our data and digital capabilities, we can deliver better and more targeted services and outcomes for the Canberra community, while continuing to unlock the value of data.

The *ACT Data Governance and Management Framework* (the Framework) supports consistent, robust data governance and management practice across ACT Government by establishing a principles-based foundation and 12 practical steps to improve how we govern and manage our data holdings. It consists of two documents:

- The **Policy Framework** provides a high-level overview of the key elements to improve data governance and management across ACT Government and is accessible for all staff.
- The **Data Governance and Management Guide** (the Guide) provides a detailed, in-depth resource to improve data governance and management practice. It will support all data users, with a focus on supporting staff with a technical aspect to their role.

The Guide

The Guide accompanies and complements the Policy Framework, providing information and detail to support you in delivering the Framework. Each section in the Guide is designed to be read on its own and as needed.

Part One – A Data Driven Culture details how we can build a data-driven culture through establishing the following foundational governance functions: our data vision and purpose; the policy, legislation and risk environment; our data principles; roles and responsibilities; and directorate data governance and management implementation strategies.

Part Two – A Managed Data Practice describes we can establish good data management processes, with the aim of improving the maturity of our data practice over time. Activities include making data discoverable; making data understood; improving data sharing; ensuring quality data; and making our data safe and secure.

Part Three - A Model to Measure Data Maturity can help us to identify where we when we begin our data journey and to measure the maturity and progress of our capabilities against the steps to govern and manage our data assets.

12 STEPS TO BETTER GOVERN AND MANAGE OUR DATA

The Framework identifies 12 steps to guide all directorates to improve our data governance and management practice. These steps can be implemented in any order to suit their readiness and maturity. This diagram signifies the desire for ACT Government directorates to incrementally build our data maturity by taking a continuous learning and growth mindset and praxis.

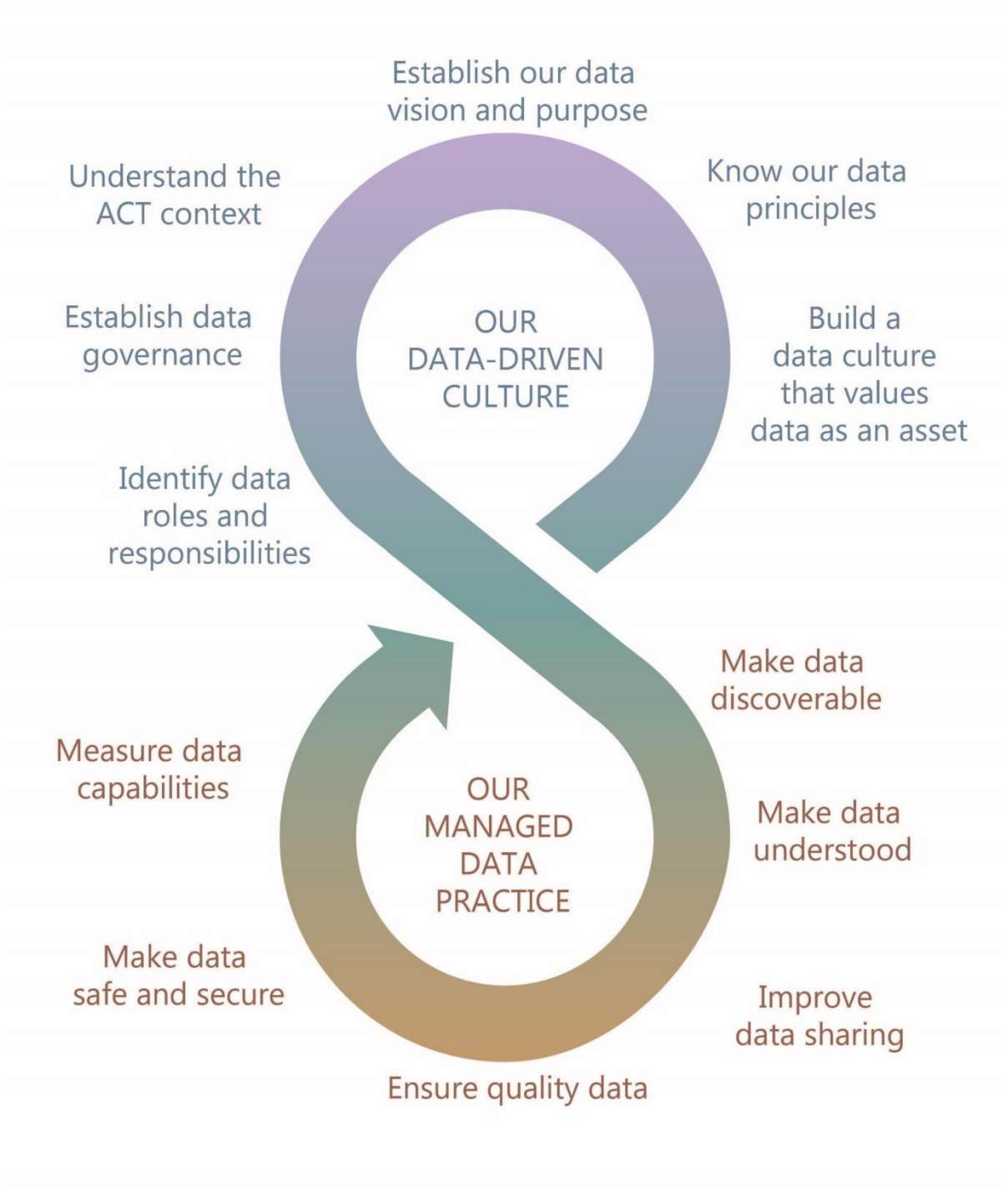


Figure 1 12 steps to better govern and manage our data in the ACT Government

Our checklist of 12 steps to better govern and manage our data in the ACT Government.

Establish our data vision and purpose

- ☐ Develop and test directorate data vision and purpose based on the ACT data vision and purpose.

Understand the ACT policy, legislation and risk context

- ☐ Understand the relevant legislative and policy frameworks, including privacy and security provisions, and current data governance and management risks.

Know our data governance and management principles

- ☐ Embed the principles in directorate data practice.

Establish data governance

- ☐ Review and re-establish data governance groups at directorate and whole of government levels.
- ☐ Develop a directorate data governance and management implementation strategy.

Identify data roles and responsibilities

- ☐ Support all staff and executives to know their role and responsibilities in working with data.
- ☐ Ensure data custodians and data stewards actively govern and manage datasets assigned to them.
- ☐ Appoint an Executive Data Lead or ensure that the function is assigned to an existing executive role.
- ☐ Support the Executive Data Lead to uplift data practice and build a data culture in the directorate.

Build a culture that values data as an asset

- ☐ Establish and promote our shared data vision, principles and values.
- ☐ Identify barriers to achieving our data vision and embedding principles in daily practice.
- ☐ Identify and foster the desired behaviours of a data driven ACT Government.
- ☐ Measure progress towards data vision and reinforce change, and then continuously improve.

Make data discoverable

- ☐ Set up data roles, responsibilities and governance.
- ☐ Identify directorate datasets.
- ☐ Identify and train data custodians and stewards.
- ☐ Register datasets in a data catalogue.

Make data understood

- ☐ Prepare business glossary for the dataset.
- ☐ Prepare data dictionary for the dataset.
- ☐ Identify primary use of the data.
- ☐ Outline data sharing rules for the dataset.

Improve data sharing

- ☐ Foster a safe data sharing culture.
- ☐ Understand the risks, barriers and challenges to data sharing.
- ☐ Understand the legislative and policy frameworks that govern data sharing.
- ☐ Establish clear, consistent governance and management practice to enable safe data sharing, including by adopting the Five Safes principles.
- ☐ Improve open data by safely releasing more ACT Government datasets on data.act.gov.au.

Ensure quality data

- ☐ Adopt a data quality framework and standard.
- ☐ Identify and document data quality issues.
- ☐ Improve data quality and resolve issues.
- ☐ Communicate quality issues and improvements.
- ☐ Ensure staff have skills and capabilities to use data.

Make data safe and secure

- ☐ Establish safe data practices, technology and controls.
- ☐ Build trust in government through safe data use.
- ☐ Support staff to know their responsibilities to implement privacy and security by design.
- ☐ Establishing directorate-level data protection, including a data breach response plan.

Measure data capabilities

- ☐ Assess our data maturity against five levels: Initiate; Develop; Define; Manage; and Optimise.

ABOUT DATA

Staff who rely on data in their work and to make decisions every day, need to be able to discover, access and use it reliably and trust its stated accuracy and timeliness over its life. This guide provides a series of management and protection processes that can be applied when capturing, storing and using data. This section defines data and its lifecycle, data governance and management, as well as how it might be used in the ACT Government.

WHAT IS DATA?

Data provides the information and evidence we need to inform decisions. We may capture original data or use data collected by other people, business areas, or organisations. Data can include administrative data, surveys, emails, voice and video files, photographs, maps and more.

'Data' is traditionally the plural form of the singular 'datum'. However, recent use has seen an increase in acceptance of 'data' used as both the singular and plural. This Framework uses data as both the singular and plural form of the noun.

Data includes observations and measurements of things and events.

- Data capture is the systematic recording, collecting, gathering or acquisition of real-world observations and measurements.
- Once captured and organised, and by applying statistical, mathematical, computational and other analytical techniques, data becomes information.
- Data and information are transformed into actionable and credible insights and evidence when they are analysed and interpreted in the context of the organisation, the key lines of inquiry or questions, and in relation to other factors and variables. This contextualised information may be referred to as knowledge.
- We use critical thinking and data and digital tools and applications to conduct the analysis and to visualise and disseminate the information and insights to users and decision makers.

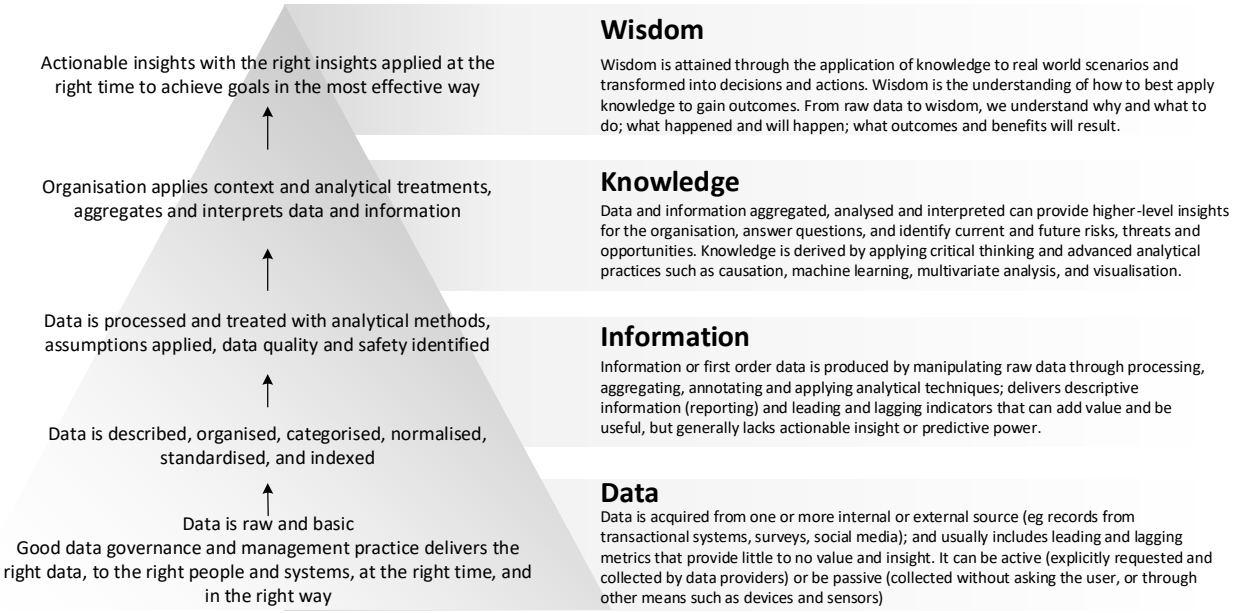


Figure 2 Informing decisions: from data and information to knowledge and wisdom

Data can be qualitative or quantitative

Quantitative data is numerical data that can be manipulated using mathematical techniques to produce statistics. It involves counting or categorising things, often placing them in a clear order, ranking or scale – i.e. nominal, ordinal, interval or ratio data. Quantitative analysis is concerned with the collection and systematic scientific investigation of quantitative properties, phenomena and relationships of data in numeric form.

Qualitative data is information in non-numeric form, which may be varied and presented in textual or narrative form. Qualitative data may include notes from observational studies, experiments or focus groups; textual responses from surveys; open-ended or in-depth interviews; and written documents. Qualitative data analysis is an iterative process of interpreting and understanding this data. It investigates the 'why' through analysing unstructured data, and contributes to understanding the how, what, where and when.

WHAT IS DATA GOVERNANCE AND DATA MANAGEMENT?

Data and analytics are becoming more central to the way we work in a digital government to drive innovation, process efficiency and automation, design new service delivery and engagement models, and build transparency and trust. However, with the growing use of contemporary data and digital approaches and technologies the ACTPS is required to build capabilities in how we govern, manage and work with data.

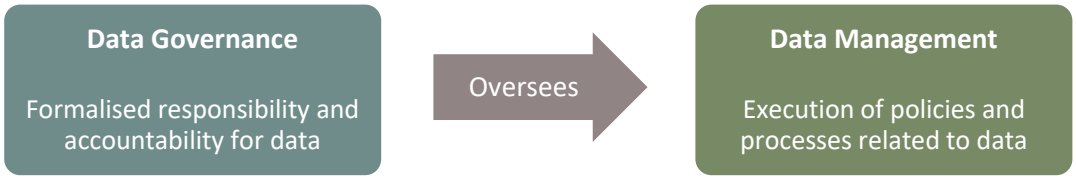


Figure 3 Data Governance and Data Management

Diagram adapted from ONDC.[1]

Data Governance

Data governance involves making decisions about how data can be captured, protected, shared and used. It ensures key staff across the ACT Government are held accountable for the appropriate handling of data and providing critical oversight of data management practices. It also represents a structured and formal commitment by the ACT Government and all directorates to take a proactive approach to building privacy and protections into the design, operation and management of our data processes and systems.

The Data Governance Institute defines data governance as "the exercise of decision-making and authority for data-related matters (and) a system of decision rights and accountabilities for information related processes, executed according to agreed-upon models which describe who can take what actions, with what information, and when, under what circumstances, using what methods." [2]

Data Governance could also refer to: organisational bodies, rules (policies, standards, guidelines, business rules), decision rights (*how we decide, how to decide*), accountabilities and enforcement methods for people and information systems as they perform information-related processes.

---

[1] Office of the National Data Commissioner (2020) *Foundational Four: guidance for agencies to improve their data practices*, available from <https://www.datacommissioner.gov.au/media-hub/foundational-four-guidance-agencies-improve-their-data-practices>

[2] Data Governance Institute, http://www.datagovernance.com/adg_data_governance_definition/, accessed 13 September 2019.

The Data Management Association (DAMA) describes data governance as "ensures data is managed properly, according to policies and best practices …(and) …focuses on how decisions are made about data and how people and processes are expected to behave in relation to data."[3]

Data Governance could also refer to: organisational bodies, rules (policies, standards, guidelines, business rules), decision rights (*how we decide, how to decide*), accountabilities and enforcement methods for people and information systems as they perform information-related processes.

Data Management

Data governance is supported by effective data management practices and processes to ensure trusted access, sharing and use of data for community benefit. DAMA describes data management as "the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets."[4]

Data management is a multidisciplinary approach to organising and handling data. It provides the foundations to make public sector data discoverable, trusted, accessible and secure. Good data management is the basis for building a data-driven culture, where the ACTPS is better enabled to realise the full value of our data assets; delivering trusted insights to underpin policy, programs and services to improve outcomes.

[3] DAMA International (2017) *Data Management Body of Knowledge (DAMA-DMBOK)*, 2nd ed., Technics Publications: New Jersey, p67-8.
[4] DAMA International (2017) p17.

DAMA Data Governance and Management Disciplines

The DAMA *Data Management Body of Knowledge* (DAMA DMBoK) identifies 11 functions or 'Data Management Knowledge Areas' that together form the foundations of good data practice. Good data governance is necessary for consistency and balance between these areas.

The Framework learns from and applies the DAMA DMBoK functions in the ACT Government context, allowing flexibility for the unique characteristics of each directorate. The Framework and Guide presents these functions into a set of pragmatic steps for directorates to the design and embed these functions in practice.

The functions are described below, with definitions drawn from DAMA DMBoK.[5]

Data governance	Provides planning, oversight, and control over the management and use of data and data-related resources. Data governance is placed at the centre of data management activities, since governance is required for consistency within and balance between the functions.
Data architecture	Defines the blueprint for managing data assets by aligning with organisational strategy to establish strategic data requirements and designs to meet these requirements.
Data modelling and design	The process of discovering, analysing, representing and communicating data requirements in a precise form called the *data model*.
Data storage and operations	Includes the design, implementation and support of stored data to maximise its value. Operations provide support throughout the data lifecycle from planning for to disposal of data.
Data security	Ensures that data privacy and confidentiality are maintained, data is not breached, and data is accessed appropriately.
Data integration and interoperability	Includes processes related to the movement and consolidation of data within and between data stores, applications and organisations.
Document and content management	Includes planning, implementation and control activities used to manage the lifecycle of data and information found in a range of unstructured media, especially documents needed to support legal and regulatory compliance requirements.
Reference and master data	Includes ongoing reconciliation and maintenance of core critical shared data to enable consistent use across systems of the most accurate, timely and relevant version of truth about essential business entities.
Data warehousing and business intelligence	Includes the planning, implementation and control processes to manage decision support data and to enable knowledge workers to get value from data via analysis and reporting.
Metadata	Includes planning, implementation and control activities to enable access to high quality, integrated metadata, including definitions, models, data flows and other information critical to understanding data and the systems through which it is created, maintained and accessed.
Data quality	Includes the planning and implementation of quality management techniques to measure, assess and improve the fitness of data for use within an organisation.

[5] DAMA (2017), pp45-46

THE DATA LIFECYCLE

Data tends to follow a general cycle over which we generate its value to inform practice and decisions. The lifecycle can be depicted in several ways and with a variety of steps and names for those steps. One example is provided below:

Figure 4 The data lifecycle

Not all steps in the data lifecycle will apply to all data and the steps do not necessarily occur in a linear fashion. For example, some data may never be released or shared, while some data may need to be shared before it can be used. The DAMA DMBOK depicts a cyclical process with additional steps to 'plan', 'design and enable', 'enhance' and 'dispose'. In another example, the Australian Department of Industry, Science, Energy and Resources *Data Strategy 2018-20* includes steps to collect, catalogue, curate, assure, store, link, share, analyse, audit, preserve and destroy.

Understanding the data lifecycle can help us to better use data in policy development. The ACT Government design wheel for policy and program development is discussed in more detail in Appendix I.

Plan and Capture	We plan the data requirements at the earliest possible phase of the activity. We collect, generate, or gather data from various sources both internal and external to the ACT Government. Data can be automatically gathered or manually inputted or entered into forms or systems through defined business processes or project activity. We must plan how the data and information we capture will meet our needs and we will be able to trust in its quality, for example by ensuring it meets quality standards. Original or primary data can be collected or generated from a variety of situations, for example: • given by an individual with their informed consent for a specific service; • provided by an individual through community consultation such as through a survey or feedback form; or • collected by CCTV networks, automatic devices, control system, or sensors. Data can be acquired from existing sources produced by another organisation. This data can be research, program or service delivery data, or information readily available via social media and open data portals. When we enter contracts with service providers or vendors that include data to be collected – for example, a contract for an external provider to deliver a service that includes collecting data on behalf of ACT Government – the data must be provided to the Territory as part of the deliverable and in an agreed format with context metadata. It is not enough for the deliverable to only include reports generated using the data. Over time, data delivery should be a standard in any procurement process and contract terms and conditions (including for government funded programs and services). When data is captured, it also needs to be organised by describing and cataloguing it to make it discoverable for wider use and reuse. We generate information about the data (metadata) so that key attributes of the data can allow for discoverability, the refined classification of data and effective analysis and use including sharing via secure platforms. To ensure consistency across ACT Government, and when designing data capture processes, consider the common data fields that should always be included and the form in which they should be captured. For example, this might include gender, Aboriginal and Torres Strait Islander status or location. This will support the ongoing development and maturity of establishing core and shared reference and master datasets for the ACT Government.

Store	We store, maintain and organise data so that it is managed inside data catalogues and storage locations that ensure the security, integrity and availability of the data. We often store data in software and databases, as well as on our computers or as documents (for example, Microsoft word and excel) on SharePoint, system or local drives. The ACTGOV network is set up to be secure for sensitive information and critical business systems, and Shared Services configures automatic backups for the systems it hosts. Staff may sometimes also use external storage devices such as laptops, removable disks or hard drives, which creates risks due to the requirement for manual back-ups and the increased possibility of being lost, stolen or damaged. During storage and maintenance, data is also processed, which may involve moving, integrating, cleansing, enriching, and extract-transform-load the data, without yet deriving any value from it. If the data is required to be current, then feedback mechanisms should be designed to ensure that there is an easy way to capture updates, with confirmation from the individual.
Use	We use data by applying it for its original purpose and through enabling its reuse and sharing for secondary and other purposes to benefit the community. There are opportunities to gain new insights from reusing de-identified data to shape policy and improve service delivery. For example, statistical analysis and visualisations can provide a robust basis for evidence-based decision making. In some instances, data can be curated to make it readily usable. Managing data quality and standards is a key part of the process from capture to use. When data is linked safely and securely with other data, it can support wider analysis. We assure datasets for quality, and audit to ensure authorised user access. Using data requires data governance measures, including being aware of relevant legal and ethical considerations, whether permissions were gained, or if there are regulatory or contractual limitations to using the data. By considering these constraints when planning and using data, we can encourage good data governance and management practices.
Share and release	We share data to authorised users and publish or release it to foster greater public benefit. By sharing data to other users in other business areas, directorates or external to the ACT Government, the data can provide greater value. By releasing data on Open Data, we enable greater transparency and can engage the community in the business of government and support the public value of data co-creation and use. However, this requires a close consideration of the purpose of the data sharing and how it contributes to public benefit, whether data users are authorised to use the data, whether the setting minimises the risk of unauthorised use or disclosure, whether protections are applied to the data, and whether outputs are also safeguarded prior to sharing or release. Ensuring good data governance provides this oversight.
Retain or destroy	We retain data to preserve it for longitudinal and timeseries analysis, accountability and historical purposes, and knowledge and decision management, or destroy it when no longer fit for purpose or corrupted. This requires the archiving of data in a secure and safe way and removing it from active production environments with a view to restore the data in case it is needed again. When data reaches its end of life, legislative instruments under the *Territory Records Act 2002* provide us with appropriate disposal schedules. Retention periods (that is, how long data is to be retained by the agency before being destroyed or retained as Territory Archives) set down in these schedule are minimum periods only and an agency may keep data for a longer period if considered necessary for business requirements. Reasons for longer retention could include legal requirements, administrative need or agency directives.

USING DATA IN THE PUBLIC SECTOR

Data helps us run the day to day operations and functions of government.

We use data in processes across the public service value stream from planning and policy design to program management and service delivery. Data also forms the cornerstone of how we manage day to day operations such as human resources and financial management.

Examples of government use of data include in service delivery such as when registering ACT road users; making operational decisions when we hire staff and contractors and managing financial transactions; generating information for planning and forecasting demand for public services; providing regular reporting such as though the Report on Government Services, and conducting research or program reviews and evaluations; and communicating and disseminating the findings.

Data can be combined with other data to improve the quality and efficiency of our operations, policies and services. Data can help monitor and evaluate the success of what we do, how we do it and the difference we make. The data we need to inform decisions is increasingly complex and rapidly growing in volume. Fast, efficient access to and analysis of government data is essential to enable better outcomes.

Government Use of Data for Public Benefit

The Office of the National Data Commissioner recognises: "Australia's data is an important national asset which can be used to inform policy development, improve service delivery and evaluate government programs.

Effective use of government data can support innovation and contribute to Australia's economic growth and social wellbeing. Sharing government data can also help to create a fairer and safer society for everyone"

For more information, visit the website and view the video on providing effective and efficient government services through using and sharing data: https://www.datacommissioner.gov.au/data-sharing/data-use

As such, there is a growing need to use quantitative and qualitative data in public services as a basis to draw robust insights and evidence to guide our decisions and ensure the effectiveness of our policies, the efficacy of our programs and efficiency of our services. When we use data and trustworthy insights to tell stories in clear, easy-to-follow language, decision makers can better understand, consider, and act upon it.

By building our capabilities to use data in our decisions, we can apply common principles and standards to:

- capture the right data on a common basis, at the right time and for the right purpose;
- combine valid and reliable data from multiple sources, across systems and regions;
- compare performance over time and/or against key benchmarks or targets; and
- communicate and report results across planning, funding, and reporting systems.

For example, by employing quantitative methods such as analytical and mathematical models, theories and hypotheses, staff can capture the appropriate and accurate measures and indicators required to identify whether an intervention or service model has successfully delivered its outputs and achieved its outcomes, and was cost effective and efficient.

Data can help answer questions like:

- What happened? When? Where?
- What or who was impacted?
- Why and how did it happen?
- What is needed, where and for whom?
- What works to deliver results and outcomes?
- What will it cost?
- How long will it take?
- What are the risks?

Qualitative methods can also be employed help validate empirical data and evidence by uncovering contextual insights into what is going on and why. They help us understand attitudes, opinions, perceptions, values, concerns, motivations, aspirations, or lifestyles, and how people, things and the community are affected by situations.

The diagram below highlights the different types of analytics processes from descriptive to predictive and prescriptive. Appendix I also provides further information on evidence-based policy and practice.

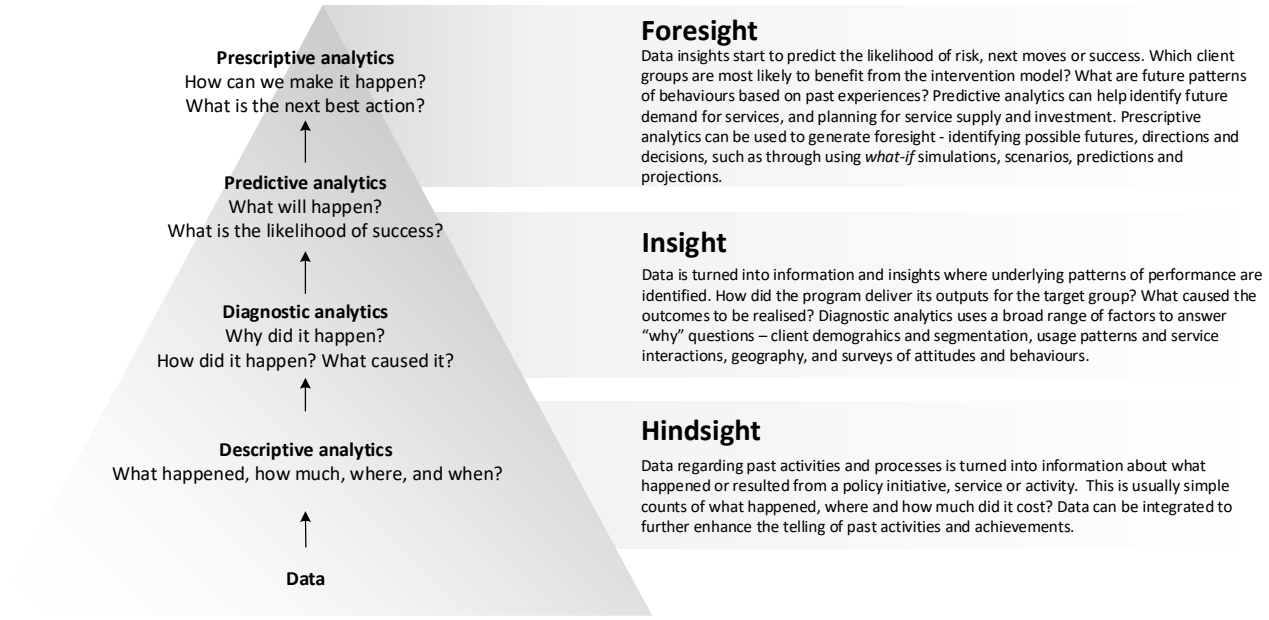


Figure 5 The Evolution of Data and Analytics – from descriptive to predictive and prescriptive analytics

Need to enhance the way we work with data across the data lifecycle

Fundamentally, the way data is captured, protected, used and shared in the public sector is changing from how it was done in the past. With enabling digital infrastructure and capabilities, data that is developed in the context of a specific policy initiative or application, can be better managed and as such safely leveraged for wider public value.

The ACTPS can modernise how we work by improving our capabilities through the application of technology along the entire data lifecycle. Although we already capture, store, use, share, release and retain or destroy data every day, the overall level of capability in realising the benefits from this data ranges from low to advance across directorates. If not addressed, a lack of consistent and mature capability can be a barrier to Canberra's ambition to be a digital city. In a very practical sense, it also significantly hampers the government's ability to efficiently deliver services in line with community expectations and limits our ability to address increasingly complex policy questions.

This Framework can help directorates to establish the foundational enablers for better data practice, particularly where personal and sensitive information are involved.

PART I – A DATA-DRIVEN CULTURE

The steps in this section helps us to build good data governance practices so that we can move to a data culture where our employees drive purpose in trusted and safe use of data

- ☐ Establish Our Data Vision and Purpose
- ☐ Understand the ACT Policy, Legislation and Risk Context
- ☐ Know Our Data Governance and Management Principles
- ☐ Establish Data Governance
- ☐ Identify Data Roles and Responsibilities
- ☐ Build a Culture that Values Data as an Asset

ESTABLISH OUR DATA VISION AND PURPOSE

1	Develop and test directorate data vision and purpose based on the ACT data vision and purpose.

The ACT Government seeks to improve the wellbeing of our people and community, so we can all reach our full potential. Public services such as schools, hospitals, transport, child protection, and community safety as well as planning, infrastructure and city services can enhance outcomes and transform the lives and livelihoods of individuals and the community. This is particularly important for people with diverse and complex needs, and for those experiencing any form of vulnerability, disadvantage or marginalisation. To foster a sustainable, resilient and vibrant community, government services are dependent on having all the relevant information to support better planning, strong decision making and effective service provision.

We **value the data we capture, protect, share and use on behalf of our community**. We want data to be captured, managed and used in a way that protects privacy and develops better services for the community. Data is a cornerstone to a truly digital government.

Our Data Vision

To enhance the wellbeing of Canberrans and visitors through safe and effective use of data in our decisions.

The purpose and importance of data governance and data management for the ACT Government

The ACT Government is committed to improving and increasing our safe use of data to support a more connected Canberra, making life better for Canberrans and the businesses that employ them.

This is demonstrated through the Open Data Policy (2015), the establishment of the Office of the Chief Digital Officer (OCDO) and ACT Data Analytics Centre (ACTDAC), and the recent moves to reform the ACT Government's information and data sharing systems and processes.

There are currently varying levels of consistency and maturity in data governance and management practice across ACT Government. To realise our data vision, we need a proactive approach that will build and strengthen data skills and capabilities, and we need to actively and diligently remove barriers for our staff to capture, protect, use and share data.

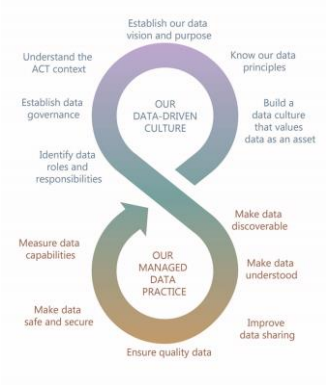
Strong, consistent data governance and management practices, supported by the Framework, will help us deliver better outcomes for our community. The diagram below demonstrates how, with consistent application of data practices and processes across all directorates, we can collectively improve ability and deliver better outcomes and improve wellbeing for our community.

ACT Government Data Vision and Purpose – Logic Map

Data governance and management practices are consistent across ACT Government directorates

The *Data Governance and Management Framework*

- articulates the data principles and common language for establishing foundational data practices and behaviours
- guides directorates to improve capabilities to safely acquire, capture, protect, use and share data
- is a living document that will evolve as we transform and mature our data and digital capabilities over time.



We value data as an asset and its potential to benefit the community

We know what data we hold and can find it

We safely and efficiently share information and data with purpose, while protecting privacy

We ensure data is fit for purpose and can be used in decision making

We protect the security and safety of data assets and build privacy into data systems and processes

We understand our roles and responsibilities and competently and safely work with data

We know, trust and use data in the decisions we make on behalf of the ACT community

We consciously learn, adapt and transform how we work using data

We earn and maintain public trust

Respectful We listen to community views and use data appropriately and ethically

Secure We proactively manage risks, protect the privacy and security of personal information

Accountable We respond quickly when things go wrong, are honest about mistakes and learn from them

Transparent We openly and proactively communicate about how we capture, protect, share and use data

Our community receives better and more targeted services, policies, planning, and research

Our community trusts that we are responsive to their needs through safe use of data

Our community trusts in government to use and protect their information

Our community is better connected and empowered to make decisions

Better wellbeing for our Canberra community

By taking advantage of advances in data and technology, the ACT Government supports our community to achieve better outcomes in health and wellbeing, safety, productivity and connectivity, supporting Canberra to be one of the world's most liveable cities

Figure 6 ACT Government Data Vision and Purpose – Logic Map

UNDERSTAND THE ACT POLICY, LEGISLATION AND RISK CONTEXT

1	Understand the relevant legislative and policy frameworks, including privacy and security provisions, and current data governance and management risks.

The ACT Government provides and funds a wide range of services for and on behalf of the community. These include education, health, housing, transport and roads, environment, business investment, and city and community services. The community sector, private sector, and the Australian Government also contribute to delivering services to our community.

ACT and national level strategies, policies and legislations guide our day-to-day work. As a result, this Framework sits within a complex ecosystem that defines how we capture, protect, share and use data. A selection of relevant legislation and policy are outlined below, noting that this is not an exhaustive list and does not include all portfolio-specific legislation that may be relevant for directorates.

Australian Government and National Legislation and Policy	*Privacy Act 1988* (Cth)	*Public Sector Management Act 1994*
	Freedom of Information ACT 2016	*Healthcare Identifiers Act 2010*
	Data-matching Program (Assistance and Tax) Act 1990	Data Availability and Transparency Bill (forthcoming)
	Public Data Policy Statement	Public Sector Data Management Project
	National data groups and partnerships including Australian Data and Digital Council and the Office of the National Data Commissioner	
ACT Legislation	*Information Privacy Act 2014*	*Health Records (Privacy and Access) Act 1997*
	Territory Privacy Principles (TPPs)	*Children and Young People Act 2008*
	Human Rights Act 2004	*Domestic Violence Agencies Act 1986*
	Territory Records Act 2002	*Crimes (Sentencing) Act 2005*
ACT Policy	ACT Digital Strategy	
	The Privacy Data Breach Management Policy: *Information Privacy Act 2014* (forthcoming)	
	The ACT Government ICT Incident Response Plan	
	ACT Government Risk Management Framework and Policy 2019	
	ACT Government Protective Security Policy Framework 2017	
	ACT Government Protective Security: Information Security Guidelines 2017	
	ACT Government ICT Security Policy	
	ACT Government Sensitive Information Encryption Standards 2020	

In 2019, directorates agreed to an information and data sharing approach of 'sharing by default except where there is a good reason not to'; thereby moving away from a widespread culture of 'if in doubt, don't.' Directorates are responsible for building an awareness and capabilities for sharing data *by default*. Over time, the ACT Government may consider introducing new policy and/or legislation to enable data sharing, like other jurisdictions. We also engage with partners in all jurisdictions to share knowledge and resources on data governance and management including data breach response, data breach notification, building trust, privacy, and data sharing.

Our current Data Governance and Data Management experiences and risks

Several common issues have been identified across ACT government relating to data governance and management. Lessons from reviews and audits have uncovered the need for adequate proactive and responsive processes and documentation to understand actions taken in relation to data safety and security risks. Together, these present a set of ongoing risks relating to data and data practice that can be better managed through implementing this Framework and its supporting resources.

Need for data-driven decisions – but data capabilities and infrastructure are varied and inconsistent

- Staff report a lack of data capabilities, systems and mechanisms that enable them to uncover compelling data insights in the right way and at the right time to inform decisions and practice.
- Executive staff have identified a need for building data analytical capabilities and leadership to inform evidence-based strategic and tactical decisions.
- Operational staff have identified the need for building internal data structures and capabilities to optimise business processes, and to free-up time and capacity for higher order tasks.
- Staff report that leaders do not prioritise and value data, and as a result do not resource the building of foundational data practices.

Need for consistency in data governance – but directorate maturity is varied

- Data governance arrangements across government are at varying levels of maturity, leading to a lack of consistent and common language about governing and managing data.
- We lack a whole of government approach to formalised data governance arrangements, based on common principles, which would drive directorate commitment and accountability.

Need for data – but people don't have visibility of datasets and don't know where to go to find it

- Directorates have identified that staff do not always know what data exists to help solve policy questions or support service delivery, both within directorates and across government.
- Staff cannot easily find quality data to reduce the burden or workload of collecting the same data.
- Directorates report that there is no consistent way of listing data holdings across government.
- Funding programs, procurement processes and contracts may not specify the delivery of data in an agreed formant with context metadata alongside procurement deliverables.

Need for data – but people can't trust it

- When staff request data, they cannot easily trust in its accuracy and completeness.
- Directorates have identified a range of data quality issues that hamper trusted data sharing and use, including inconsistent or missing data definitions, physical addresses not being validated for accuracy, misspelling of names of people or suburbs, and missing values such as for gender and Aboriginal and Torres Strait Islander status.
- Directorates report an absence of whole of government common data and data definitions, hindering the ability to combine and compare datasets and to gain trusted data insights.
- Data custodians are not always aware of their role in ensuring and improving data quality and useability.

Need for data and consistency – but systems lack consistency

- Data is contained in legacy information technology systems with a lack of common data definitions or standardisation between data systems, no provision of metadata and inconsistent storage formats.

- Need for business systems tend to be funded based on business cases and can often be designed for the specific needs of the business functions, thereby missing opportunities to leverage combined and whole of Government requirements and capability.
- Staff may inadvertently duplicate data or replicate information when saving files in shared drives or emailing data files.
- Staff may acquire and manage data in the context of single business functions, thereby missing opportunities for further value creation in the whole of Government context and limiting the ACT Government's ability to realise the goals of "One Government" and "Open Data".

Need for data – but people don't know how to use and work with it

- While some directorates have areas of advanced data analytical capabilities, overall staff report lower confidence in data capabilities and data literacy.
- Directorates identified the need to build staff data analysis skills, that is, ability and capabilities to:
    - work with data, link it with other data, visualise it, interpret it and tell stories with it;
    - identify the right questions and methodological approaches to analyse data;
    - move from basic analytical approaches to advanced analytical methods such as data linkage and integration; and
    - understand privacy and confidentiality of data, as well as safe sharing and use.
- Directorates also acknowledge the growing interest in publishing data on the ACT Government open data portal (data.act.gov.au), however require support to ensure data is safe for public release.
- Directorates acknowledge the need to build confidence and trust in data governance and data and digital literacy both within directorates as well as with the community.

Need for Safe and Secure Data practice – but it's hard to accept that it is everyone's responsibility, because people still aren't sure what that responsibility is

- There is an absence of a whole of government Data Security Strategy, with tactical and operational implementation of data security being fragmented and inconsistent across directorates.
- Some see data security strategy as a 'feature' or an 'extra cost' in the design of data systems, rather than a core requirement.
- Fragmented and inconsistent data security implementation limits whole of government understanding and management of information and data security risks.
- Current risk management approaches to data security often require complex assessments that may not be easily understood by staff without a technical cyber security role. To be effective, risk assessments must be regularly tested and updated against an evolving threat environment. The expertise required to perform and test these assessments creates a backlog of risk assessments within Shared Services ICT Security.
- Where risks management can be undertaken by other staff, there is often a lack of understanding and experience about data security risks and whose responsibility it is to manage them. This can lead to a 'tick the box' culture; which accepts vendor assessments of whether a product or service is safe and does not require directorates to ensure that their risk controls are performing the actual risk reduction they are supposed to, or that they are up to date for an evolving threat environment.
- There is a lack of consistent data breach reporting standards and mechanisms communicate to the community and build the community's trust in government
- Directorates have identified the need for comprehensive data security training to support staff to understand data security risks and their corresponding responsibilities around protecting personal data.
- Directorates have identified a need for safe and secure data sharing but may not ensure data is safe in their internal systems.

Need for data – but people either don't know if it can be shared or can't access it

- Data sharing is a significant challenge within and between directorates, with staff reporting a mix of behavioural, cultural, technical and legislative barriers to data sharing.
- Staff report a genuine lack of understanding about whether the data can be shared, for what purposes, with whom, and how, with this varying level of uncertainty leading to staff and executives being risk-averse.
- Staff may be unaware about whether consent has been gained for sharing personal information and, when consent is gained staff may be unaware of the provisions of sharing data or unsure whether the data can be shared for purposes other than that for which it was collected.
- Directorates identify the need for greater clarity on the potential for data to be re-used for research, policy and strategic planning purposes.
- Provisions relating to data sharing, how that data can be used within ACT Government and whether it can be released under Freedom of Information may not be clear or well understood by stakeholders within data sharing agreements, contracts or memorandum of understanding.
- A risk averse culture that impedes the sharing and reuse of data due to
    - longstanding experiences and a lack of understanding about whether data can be shared
    - poor quality of the datasets and mistrust in the capabilities of data users
    - mismatch between community expectations to share data and a fear of undermining trust
    - few direct consequences for withholding data even when there is a legal basis or community expectation to do so, and fear of repercussions for inappropriate disclosure or use.
- A complex legislative environment within directorates and across government can make it difficult for individuals to understand whether data can or can't be shared.
- Inconsistent governance and policies within directorates and across government preventing staff from confidently making decisions to share information and data.
- Outdated digital infrastructure where data is manually extracted, cleansed and shared through outdated and unsecure mechanisms.

KNOW OUR DATA GOVERNANCE AND MANAGEMENT PRINCIPLES

Embed the principles in directorate data practice.

Figure 7 ACT Data Governance and Management Principles

The Framework presents the case for taking a principles-based approach to data governance and management within and across ACT government directorates and agencies. Eight principles were codesigned as our key values and goals by staff representing their directorates from across the ACT Government. When these are applied, directorates can ensure data practices are fit for their specific purposes and unique contexts, while building a more consistent and comparable approach across government.

In developing these principles, consideration was given to the specific data governance challenges facing ACT Government as well as alignment with existing strategies, policies and service delivery contexts. At the national level, the Australian Data and Digital Council's four trust principles and the Office of the National Data Commissioner's data sharing principles were also considered.

By taking a principles-based approach, the ACT Government recognises that directorates are all at different stages of their data governance and management journeys. This approach will support directorates to develop directorate or agency-specific data governance and management implementation strategies and roadmaps (further information on this step is in the 'Establish Data Governance' chapter).

We are community-centred	• We actively and respectfully engage with the community to understand and address their needs and concerns about the data we capture, protect, share and use on their behalf.	**We make data discoverable**	• We know what data is available and how to find it by ensuring data is clearly and explicitly described and registered in a searchable resource.
We are transparent and accountable	• We openly and proactively provide clear, accessible information to the community about how we capture, manage use, and share data. • When things go wrong, we respond quickly, are honest and learn from our mistakes.	**We make data trusted and secure**	• We make data quality known and manage data integrity and consistency. • We are proactive in protecting the security of the data we capture, protect, share and use on behalf of the community.
We share and use data safely	• We share data to benefit the community, while proactively protecting the privacy of individuals. • We ensure appropriate and ethical use of data, in accordance with legislative and policy requirements.	**We value data**	• We use data to inform evidence-based policies, programs and services that improve outcomes for our community. • We treat data as an asset because we recognise the potential of data to benefit our community.
We are skilled and capable	• Our staff are empowered with appropriate skills, knowledge and capabilities to work with data. • Our staff know their responsibilities and obligations to ensure safe and trusted capture, use and sharing of data.	**We make data open**	• We make ACT Government data freely available for public access and use to support community wellbeing, innovation and growth.

ESTABLISH DATA GOVERNANCE

1	Review and re-establish data governance groups at directorate and whole of government levels
2	Develop a directorate data governance and management implementation strategy and roadmap

Data governance and management principles

We are community centred	**We are transparent and accountable**	**We share and use data safely**	We are skilled and capable
We make data discoverable	**We make data trusted and secure**	**We value data**	We make data open

This section supports directorates to take a consistent approach to establish data governance arrangements to oversee the way we capture, protect, share and use data to benefit our community.

ACT data governance arrangements and structures

By establishing robust data governance arrangements, we can improve the visibility and availability of data, create the foundations for fostering a data-driven and evidence-informed ACT public service, and demonstrate that we value the data we capture, protect, share and use on behalf of the community. With effort, strong relationships and shared accountability, we can foster a collaborative data governance and management system in the ACT Government.

There are four components to good data governance arrangements:

- Embedding our **data governance and management principles** (page 29)
- Establishing **data governance groups** to be accountable for how data-related decisions are made
- Developing a directorate **data governance and management implementation strategy** and **roadmap**
- Clarifying and assigning **data roles and responsibilities** (page 43).

By having these critical governance arrangements in place, directorates can establish a compelling mission for transformational change, mobilise our change leaders, staff and resources, win over hearts and minds towards a common values-based data culture and behaviours, and drive momentum through iterative action and reflection, monitor how the directorate is making progress, and share lessons and successes.

Directorate Data Governance and Management Implementation Strategy and Roadmap

It is important that directorates have a strategy to manage data assets in the same way that directorates develop strategies to manage and use other resources and assets (such as a corporate or a workforce strategy).

To effectively improve data maturity, each directorate is required to establish a data governance and management implementation strategy (a Data Strategy). This strategy will help directorates to shape our data journeys and maturity, while ensuring directorate data practice are consistent with the whole of government *Data Governance and Management Framework*, which includes this Guide.

What is a Strategy?

A Strategy is the art of applying resources in the most effective and efficient way to achieve an agreed and firm position, by:

- defining clear objectives, direction and goals to back up the position.
- creating advantageous conditions through and specific and targeted actions.

Having a directorate-level Data Strategy will:

- help executives, staff and partners to establish a common vision and paint a clear and common picture of desired future-state what does a data-driven directorate look like;
- determine a compelling case for change from discovering why improving data governance and management matters to us all and focus on identifying the most effective way to win over hearts and minds, i.e. how might we connect with people at all levels to make the desired values and behavioural changes, what needs to be true today that we will need to challenge, what success will look like and how will we measure success;
- provide a clear commitment and plan of action to achieve the desired change including through establishing internal data governance structures and data management processes;
- help change the way data is seen in the directorate, from an 'IT issue' to a way of doing business that is part of the role of all staff and contributes to decision-making at all levels; and

- support improved data sharing within and between directorates, help with understanding the barriers to data sharing (including technical, cultural and capability barriers) and provide a strategy to remove those barriers.

An outcome-based Data Strategy might consider the following four key outcome areas:

1. **Our People** are capable and empowered to thrive in a culture that values data as an asset.
2. **Our Processes and technology systems** enable us to govern, manage, use and share data.
3. **Our Governance structures** and **leadership** demand data insights to inform our decisions with open transparency and accountability to the community we serve.
4. **Our Maturity model** and approach to change is driven by measuring progress against a capability model, learning from failures, celebrating successes and applying a growth mindset.

Developing a Data Strategy

Prior to designing a Data Strategy, we will need to consider and answer the following questions:

- Why do we need a data strategy?
- Will it be a standalone strategy or form part of another directorate strategy (eg strategic plan, business plan or corporate strategy)?
- Who might we consult with to inform all aspects of the strategy?
- How do we establish a vision for the future?
- How do we gain support and buy-in? (including any resources and funding)
- What is the structure of the strategy?
- What will be included in the strategy? (e.g. people, process, technology, governance activities)
- What materials will need to accompany the strategy?
- How will we implement the strategy?
- How will we monitor and evaluate our implementation of the strategy?

Appendix II provides a further guide on how to develop a directorate Data Strategy.

The following table provides the key steps needed to design a *fit for purpose* Data Strategy in ACT Government Directorates.

Establish	Mandate and charter, governance arrangements, reference groups
Review	Context, current & past strategies, implementation & change experiences
Consult	Staff, executives, stakeholders, community, other orgs – go wide, big!
Identify	Lessons: what worked, what didn't work, new opportunities, gaps
Produce	Report: "What we heard" + ideas, pressure points, challenges, needs
Prepare	Discussion paper, communications artefacts – blogs, newsletters, FAQs
Define	Strategy design principles – specific to lessons and context
Engage	Staff to contribute to design the strategy – make this fun! Discuss their work, future vision, objectives and actions, desired culture
Propose	Vision, mission, change themes and actions, change management, success and roadmap (continue, start, explore), and maturity model
Engage	Staff and executives on final Strategy, gain buy-in, gain investment, community change
Share	Over time, staff stories of what the vision and mission means to them and what actions are taken / would take to help to make this a reality

From the first four steps we will have:

- Gained the authorising environment in which to develop the Data Strategy and change journey.
- Consulted with experts, staff, partners and clients to uncover the current data analytics, governance and management experience, practices and maturity, understand what is working, and the current challenges and barriers to a mature data practice.
- Identified clear focus areas and a set of activities and measures to achieve our vision and mission.

From this we can:

- identify ways to address common barriers to data maturity such as legislative barriers, process and technical capabilities, staff capabilities and culture, governance and leadership;
- identify the strategic, policy, program and service delivery questions and performance outcomes that data can help answer or support;
- identify the directorate's vision for data that aligns with strategic objectives and priorities, including a compelling account of "why" data is important to us and how we will work to improve our data maturity;
- articulate this as a transformational change journey to build the directorate from a current state of low data maturity to a data-driven culture that supports continuous learning and improvement;
- identify an implementation approach for the Data Strategy, outlined in the roadmap, which may include a schedule, project plans, change management, communications and engagement plans;
- identify what success will look like and how we will communicate the Strategy, the vision and the desired change, as well as stories of progress and change, with all stakeholders; and
- identify and communicate what a successful Data Strategy will look like for our directorate – i.e. What will success look like when applying this Framework in context and practice? How will we monitor and evaluate progress?

Implementation Roadmaps

An **implementation roadmap** can help us to mobilise our change leaders, staff and resources to drive change and build staff mindset based on agreed values and ways of working.

The roadmap should be simple, with the goal to iteratively implement the 12 steps over time, drive momentum through action and reflection, monitor how the directorate is making progress, and share lessons and successes.

When establishing activities and how they will be implemented, our roadmaps should consider the 'now', the 'next' and the 'beyond'. Each stage will need to respond to challenges, changing environments, shifting community expectations and emerging data and digital technologies.

What is a Roadmap?

A Roadmap is the high-level plan to help us achieve our defined and desired objectives, goals and outcomes.

It includes the major steps and milestones, on a timeline, that will help us to achieve our objectives.

A Roadmap provides a useful way of communicating our strategic goals and visualise how we will get there.

The '**now'** involves solving existing barriers and issues though continuing, enhancing and improving existing good data practices, increasing efficiency and maximising the value of our data assets and resources. The '**next'** takes us towards preparing for the future by identifying new ways of using data in our operations, building a community-centred culture of data and innovation, integrating and using data and digital technologies and increasing diversity and inclusiveness in our staff. The '**beyond'** is about exploring the new ways of working with data and preparing to adapt and thrive in an uncertain future that will be more data-driven, connected, networked and fluid.

Our roadmaps should consider activities from all these dimensions – 'now', 'next' and 'beyond' – at each stage of implementation. It should not wait, for example, for the third year of activities to implement

activities focused on 'beyond'. The following sample graphic depicts a way that we may choose to map out the 12 steps and supporting activities, processes, tools and resources.

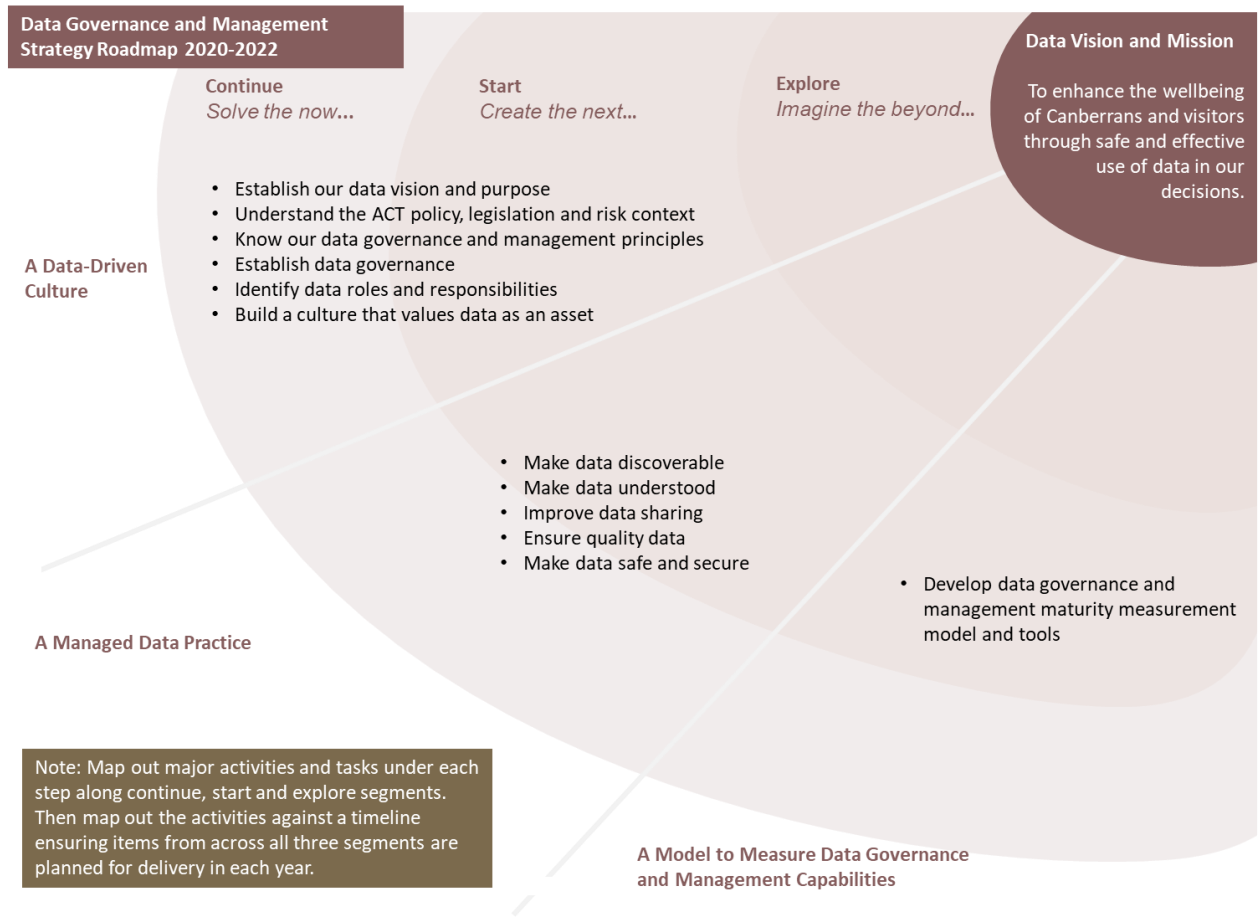


Figure 8 Data Governance and Management Sample Roadmap Graphic - Continue, Start and Explore

Common reasons why data governance and management initiatives and activities fail

Aim to avoid the following common pitfalls when implementing our data strategies and roadmaps:

- lack of understanding of the importance of data governance and management to support valuable and trusted data insights and decision-making;
- lack of funding and resources allocated to data governance and management – e.g. "to resource data governance and management, we need to take people and funding away from the front line";
- lack of commitment including top level executive support and championship;
- not seen as an organisational risk, not prioritised and not part of organisational strategy;
- too hard to do, takes too long, staff don't know how (e.g. data modelling);
- lack of consistency in roles and understanding including in data architecture and data sharing; and
- lack of communicating expected change and ongoing measurement of progress.

What does data governance and management success look like?

Target the following common success factors when designing and implementing data strategies:

- Assign clear accountability for data governance and management at executive and operational levels
- Directorate Data Strategy and/or other organisational strategies and plans provide common data vision and commitment to
    - value data as a corporate asset to inform decisions, strategies, and goals
    - build data culture, practice and maturity
    - embed ACT data principles and framework

- acknowledge data risks including safety and security in corporate risks
- Directorates and whole of government structures and arrangements take a disciplined and pragmatic approach to improving data practice and capabilities
- Staff have data as a core part of their work eg job descriptions identify executive data lead, data custodian, data steward, and data user responsibilities
- All executives, leaders and staff improve data literacy and capabilities
- Ensure consistency in data practice and operations across the ACT Government.

Whole of Government Data Governance Groups and Committees

Data governance arrangements for the ACT Government and directorates are founded on the notion that good governance is manifested in accountable decision-making, where staff acting across the strategic, tactical and operational layers can lead the desired change to achieve better data practice. The desired change is outlined in the logic map in the 'establish our data vision and purpose' section of the Framework.

A cascading data governance model across these levels is depicted in the diagram and table (below). As the ACT Government builds its data capabilities, it will continue to review these for fitness of purpose and context. It is recommended that staff understand the whole of government data governance structures when planning each directorate's approach to data governance.

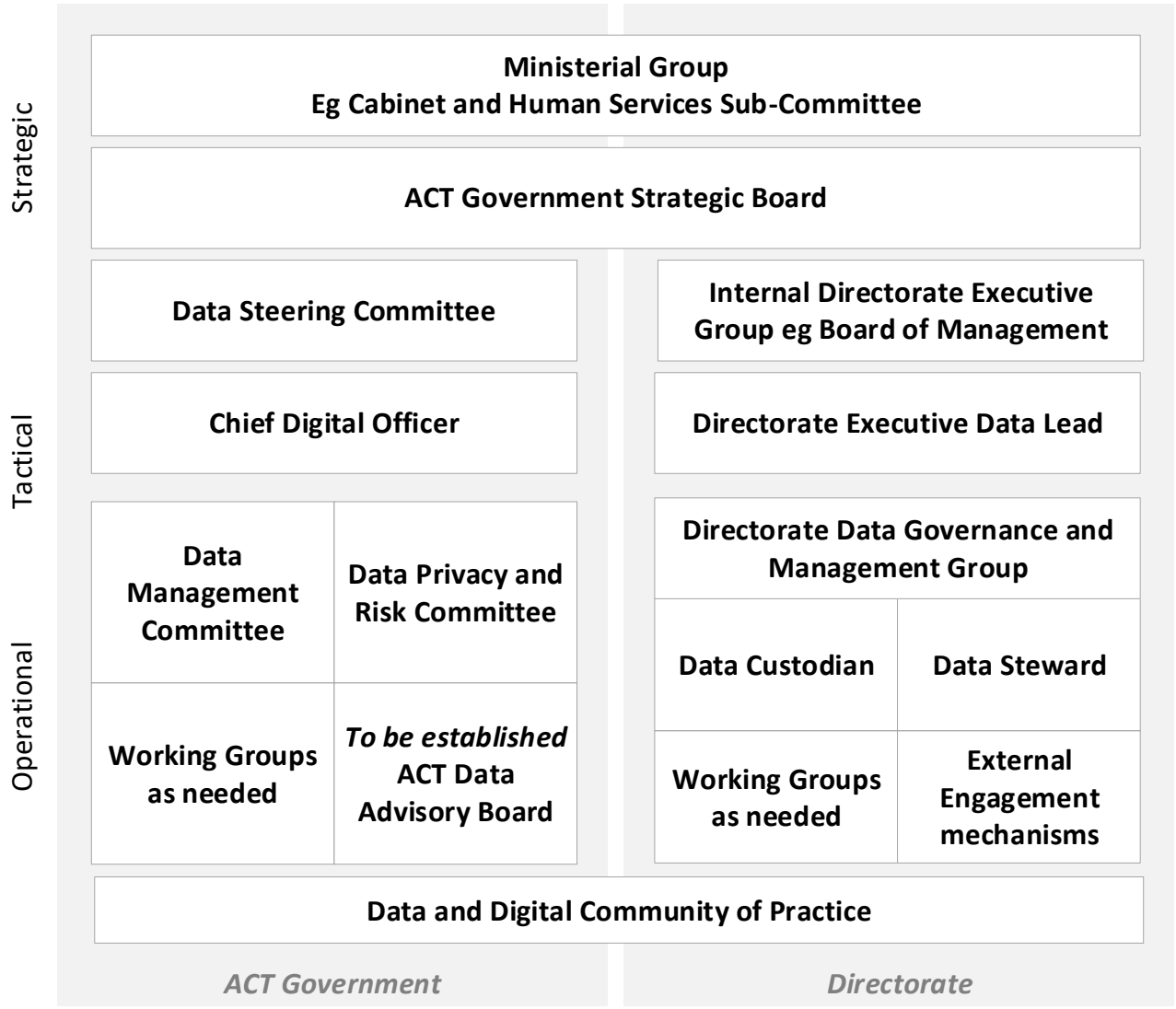


Figure 9 ACT Government and Directorate Level Data Governance Groups and Committees

<table>
<tr><th></th><th></th><th colspan="2">ACT Government*</th><th colspan="2">Directorate</th></tr>
<tr><td rowspan="2">Strategic</td><td rowspan="2">High level oversight of data practice
Address systemic barriers
Allocates resources to strategic priorities and innovative enablers</td><td colspan="2">Strategic Board</td><td colspan="2">Directorate Executive Board</td></tr>
<tr><td colspan="2">Provides whole of Government leadership and strategic direction for Data Governance and Management in the ACTPS.
Fosters data culture across the ACTPS
Membership includes the Directors-General of all ACT Government directorates, and other Executives as appointed.</td><td colspan="2">Provides leadership and strategic direction for the Directorate.
Membership includes the Director-General, Deputy Directors-General and other Executives as appointed.</td></tr>
<tr><td rowspan="2">Tactical</td><td rowspan="2">Active oversight of data practice
Identify risks, issues and remove barriers through innovation
Plan, coordinate and apply resources including data infrastructure, and resources</td><td>Data Steering Committee</td><td>Chief Digital Officer</td><td>Data Governance Committee</td><td>Executive Data Lead</td></tr>
<tr><td>Leadership to monitor, protect, prioritise and develop the ACT Government's data assets.
Allocates resources across data projects and data ecosystem</td><td>Drives data and digital transformation
Accountable for guiding consistent data practice
Point of escalation for cross directorate data issues
Oversees the work of ACTDAC</td><td>Align with ACT Government strategic priorities.
Sets directorate data priorities and roadmap
Oversees directorate data management practice improvement</td><td>Builds data and digital culture
Implements Data Governance and Management Framework.
Point of escalation for data risks and issues within directorate.</td></tr>
<tr><td rowspan="4">Operational</td><td rowspan="4">Day to day operations to achieve outcomes and maintain continuous improvement
Ensure consistent data governance and management within Directorate and partners
Manage operational risk, monitor performance and compliance, and escalate barriers</td><td>Data Management Committee</td><td>Data Privacy and Risk Committee</td><td>Data Custodian</td><td>Data Steward</td></tr>
<tr><td>Develops and guides implementation of the ACT Data Governance and Management Framework.
Contributes to whole of Government data governance and management activities eg master data management and data analytics platform.</td><td>Examines, advises and/or coordinates whole of Government approaches to address risks associated with legal, privacy and ethical considerations for data use, sharing, retention and disposal.</td><td colspan="2">Subject matter experts driving execution of the framework, strategy and roadmap in their line areas.
Other roles identified in this document also support the framework execution.</td></tr>
<tr><td colspan="4">Data Community of Practice</td></tr>
<tr><td colspan="4">Data novices, specialists, practitioners, leaders and people interested in data come together to share ideas, solve problems, connect with peers, and build capabilities.</td></tr>
</table>

*The ACT Government data governance arrangements will be reviewed from time to time to ensure we keep abreast of the changing data ecosystem, changes in government context and directions, as well as to meet community expectations.

All directorates are required to actively engage and participate in the whole of government data governance groups.

Strategic Board

The ACT Government Strategic Board provides whole of government leadership and strategic direction for the ACTPS. In a data context, Strategic Board fosters a data culture and supports safe data use across the ACTPS while providing high level oversight of the implementation of the *Data Governance and Management Framework*. Membership includes all ACT Government Directors-General.

Data Steering Committee

The Data Steering Committee (DSC) implements our data vision and drives our ambitions to fully leverage the value of our data holdings. The DSC builds data analytics capabilities and implements whole of government data governance and management policies and practices.

The DSC is the most senior data governance group in the ACT Government, providing strategic direction, leadership and advice on the prioritisation, development and management of the ACT Government's data assets. The DSC plans, coordinates and allocates resources across the ACT data ecosystem including data analytics projects, data infrastructure and data capabilities.

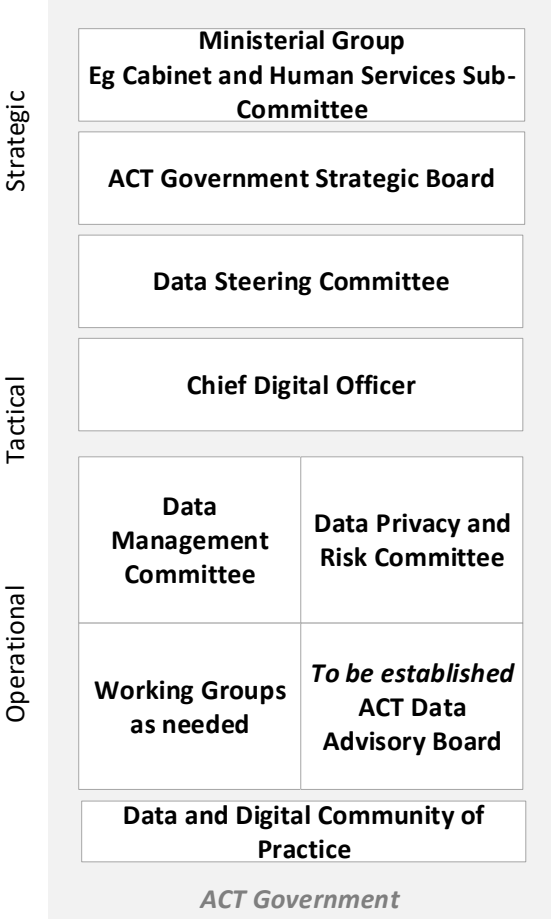


Figure 10 ACT Government Level Data Governance Groups and Committees

The Strategic Board appoints a Director-General as chair of the DSC. DSC membership is drawn from across government, ideally at Deputy Director-General level (or their delegate), to provide both executive accountability and a spread of insight and expertise.

Data Management Committee

The Data Management Committee (DMC) was established by the DSC to develop and implement the ACT *Data Governance and Management Framework* (this framework). The DMC supports directorates to apply the data practices outlined in the. The DMC examines any issues referred to it by the DSC or by its members relating to data governance and management, and data analytics technologies and platforms.

Membership of the DMC is drawn from across all ACT Government directorates, with each member responsible for championing the implementation of this Framework in their directorate. The DMC may establish time-limited working groups to create resources, tools and materials to accompany the Framework.

Data Privacy and Risk Committee

The Data Privacy and Risk Committee (DPRC) was established by the DSC to examine, advise on and/or coordinate whole of government approaches to address risks impeding our use and sharing of data. The DPRC considers issues referred to it by the DSC or by its members relating to the risks and barriers associated with data privacy and ethics rather than technical, operational or project-specific risks.

Membership of the DPRC is drawn from across all ACT Government directorates.

Data and Digital Community of Practice

A Data and Digital community of practice is emerging in the ACTPS with members from all directorates coming together to share stories of data use, barriers and analytical approaches. Members build connections, informal partnerships and support, and establish collaborations without ACTDAC involvement.

Office of the Chief Digital Officer

The Office of the Chief Digital Officer (OCDO) and the ACT Data Analytics Centre (ACTDAC) support directorates to implement consistent data governance and management practices.

The OCDO was established in 2015 to drive the ACT's digital agenda and lead the whole of government strategic direction for ICT. The OCDO reports directly to the Head of Service and the Chief Minister, Treasury and Economic Development Division (CMTEDD) and works with the ACTPS Strategic Board (comprising all Directors-General) to ensure whole of government solutions.

ACTDAC was established in 2018 to provide an ACT-wide data analytics capability and help improve the management, use and reuse of government data to create public value and benefit. This enables directorates to improve data analytics, enhance evidence-based policy decisions and deliver better services.

ACTDAC supports directorates to improve data governance and management practices, enabling safe and trusted sharing and public release of government data assets.

ACT Government ICT Committees

This framework signals the importance of connecting data with digital functions. As such, the ICT governance groups that oversee and monitor the risks and return on ICT investment and delivery, also have a role to support implementation of this framework. These include the Digital Services Governance Committee, the Geospatial Advisory Sub-Committee and the Architecture Design Review Panel. Further detail on whole of government groups and committees is provided in the *Data Governance and Management Guide*.

The **Digital Services Governance Committee** (DSGC) is the most senior ICT committee in the ACT Government, providing strategic direction, leadership and advice on prioritisation on the development and management of the ACT Government's information and technology assets. Membership of the DSGC is drawn from across government to provide a spread of insight and expertise and may not include a representative from all ACT Government directorates.

The **Geospatial Advisory Sub-Committee** (GASC) reports to the DSGC and is responsible for ensuring ACT Government spatial data is governed appropriately and supporting spatial data management to ensure data is high quality, reliable, easily discoverable and readily available in a range of formats.

The **Architecture Design Review Panel** (ADRP), in collaboration with technical subject matter experts, review the ICT / digital system solution design against a whole of government approach. The ADRP has a role to ensure data, privacy and security are embedded in the design and decisions of data architecture and solutions, including agreeing to standards and standard definitions for data management.

Directorate Data Governance Arrangements

Ensuring good data governance within directorates will involve establishing the appropriate leadership and accountability structures to support governance arrangements and that are fit for the directorate's context, including within directorate agencies. Directorates should:

- identify and establish internal data governance bodies to oversee the implementation of this framework;
- develop policies and procedures for data use and management in accordance with the ACT data governance and management principles;
- establish directorate data governance and management implementation strategies and roadmaps;
- identify and appoint people with data-specific roles and responsibilities to support data governance, management and use; and
- foster a data culture, build staff capabilities and manage change.

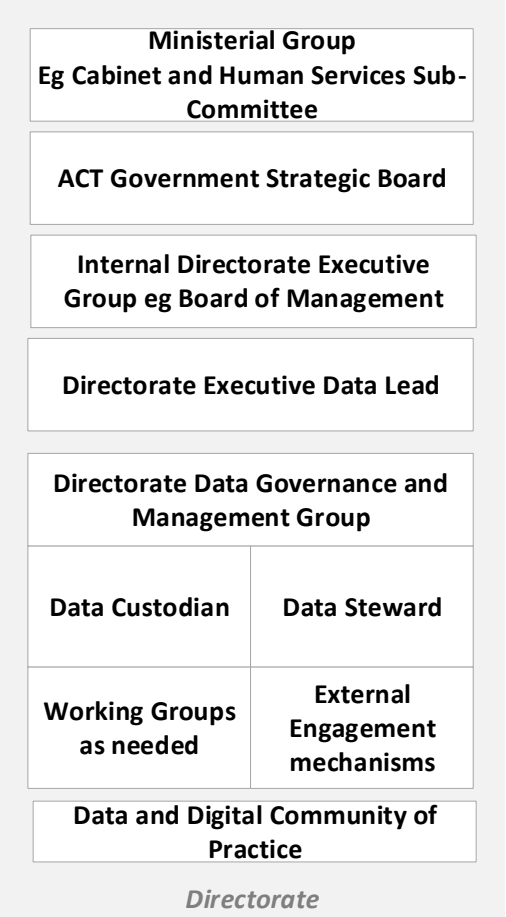


Figure 11 Directorate Level Data Governance Groups and Committees

Establishing directorate data governance bodies

Each directorate will decide its individual approach to data governance bodies.

Directorates may choose to refresh existing or establish new data governance bodies or groups to provide oversight and governance.

Membership of data governance bodies will include the directorate's Data Executive Lead, data custodians and data stewards, and other directorate executives and staff as needed.

Directorate data governance bodies will be responsible for developing and implementing a **directorate Data Governance and Management Implementation Strategy and roadmap**, which will embed the data governance and management principles and guide directorate data governance and management practice (further information below)).

It is important that data governance within the directorate is supported at a senior executive level to foster a data culture within the directorate, develop buy-in from staff, build accountability for safe and trusted use and sharing of data, and ensure successful implementation of the directorate Data Strategy.

Resources

to support work to establish data governance

- The Australian Institute of Health and Welfare (AIHW) was established in 1987 as an independent corporate entity under the Australian Government health portfolio. The AIHW's Data Governance Framework identifies and provides an overview of the AIHW's robust data governance arrangements, including:
    - a description of key concepts in data and data governance;
    - the legal, regulatory and governance environment in which AIHW operates;
    - core data governance structures and roles;
    - an overview of AIHW data-related policies, procedures and guidelines;
    - systems and tools supporting data governance; and
    - compliance regimes.
- The internal data management functions outlined are defined by the Data Management Association International (DAMA DMBOK 2007):
    - data architecture management — entails defining the blueprint for managing data collections
    - data development — comprises analysis, design, implementation, testing, deployment and maintenance
    - data operations management — relates to the provision of operational and technical support from data acquisition to purging
    - data security management — deals with matters of privacy, confidentiality and appropriate access
    - reference and master data management — involves managing information on standards and the business of the organisation
    - data warehousing and business intelligence management — enables reporting and analysis
    - document and content management — relates to managing data held outside of databases
    - metadata management — integrating, controlling, and providing metadata
    - data quality management — defining, monitoring, and improving data quality
- AIHW (2014b) https://www.aihw.gov.au/getmedia/0d59ee71-9abe-4806-8e87-ce9de81974d3/AIHW-data-governance-framework.pdf.aspx
- A more detailed guide to assist in creating a fit for purpose Data Strategy and roadmap to data governance and management maturity for each directorate is provided at Appendix II.

IDENTIFY DATA
ROLES AND RESPONSIBILITIES

1	Support all staff and executives to know their role and responsibility in working with data.
2	Ensure **data custodians** and **data stewards** actively govern and manage datasets assigned to them.
3	Appoint an **Executive Data Lead** or ensure that the function is assigned to an existing executive role.
4	Support the Executive Data Lead to uplift data practice and build a data culture in the directorate.

Data governance and management principles

We are community centred	**We are transparent and accountable**	**We share and use data safely**	**We are skilled and capable**
We make data discoverable	**We make data trusted and secure**	**We value data**	**We make data open**

Understanding who is accountable for good data governance and management within directorates is key to successfully implementing good data practices and helps improve the consistency of our data governance and management across government.

By default, all ACT Government staff are **data users** and are responsible for their own safe and appropriate use of data. Some staff have additional functions with responsibility for good data governance and management, including **data custodians**, **data stewards**, **system owners** and directorate **Executive Data Leads** (or **chief data officers**). Directorates carry other functions that contribute to good data governance and management, including privacy, data and ICT security and records management.

Data Providers

As data users, we have a responsibility to safely manage the data we hold and use on behalf of the community and those who provide the data to us. Data ownership is a complex issue and data collected or held by government does not grant ownership or proprietary rights, except in limited cases. We must always be aware of our responsibilities to protect personal or sensitive information and to use it for community benefit. Personal information may relate to an individual, household, business or other entity and is subject to a range of protections under privacy and portfolio legislation.

Consumer Data Right (CDR) gives consumers greater control over their own data, including the ability to securely share data with a trusted third party. This concept of consumer control is central to the CDR framework which gives consumers the ability to direct data holders to provide their data to accredited data recipients for example to other banks and fintechs. The regime was designed to enable more choice for consumers in where they take their business, or more convenience in managing their money and services. Informed consent is key to this choice. The Australian Competition and Consumer Commission (ACCC) is responsible for implementing the CDR system, accrediting providers and enforcing the CDR Rules. Strong privacy protections are built into the system and will be enforced by the OAIC and the ACCC.

Data Users (all ACT Government staff)

We are all data users. In one way or another, we all engage with data and information derived from data to inform our work - from a nurse monitoring patient heart rate on a hospital ward, to a program officer running a community engagement activity, a policy officer providing recommendations in a brief or an executive making funding decisions. Using data is not solely the responsibility of data or ICT professionals.

Some of us may capture data as a regular part of our work, or data may be automatically generated as we perform our daily tasks using data and digital tools and systems. Data we gather might be about the people and community we serve, or about the buildings and infrastructure that we help build and maintain across the Canberra community. We work with data throughout the data lifecycle to provide timely and appropriate supports directly to clients, creating insights to inform policy decisions, managing the strategic direction of government projects and priorities, and ensuring the security of our information and technology systems.

D**ata users** can be defined as data producers or data consumers. Some staff may be both.

A **data producer** captures and stores information. For example, someone in a service delivery role who captures information about clients is a data producer.

A **data consumer** receives information that for analysis, share or use to inform decisions. For example, the same person in a service delivery role, when using information about clients to improve services, is a data consumer.

Data users and their managers are responsible for appropriate and safe use of data in compliance with relevant policies and legislation. All data users are responsible for their own data learning and development. Sometimes we have authorisation to use data because of our role. Sometimes, we need to seek authorisation by providing a required set of information to data custodians and data owners.

How might using data be a part of our role?

Data is generated and used for a range of purposes across the ACTPS, including to inform policy development, provide more tailored services, evaluate the effectiveness of government programs, ensure compliance with laws and regulations and conduct research to improve the wellbeing of our community. By using data in our work, we can work faster and smarter and be more confident in making more precise and accurate decisions to deliver better quality government services and programs.

There are many ways that we can use data, and these will differ depending on our role. For example, a policy officer will use data differently to a program manager or service delivery staff, with different processes and tools. The table below provides some common examples of data use.

Examples of data use	What might this look like?	Example
Accessing and reading data	Looking at information and being able to understand what it means for our work, the work we are doing, and our clients.	Service staff working directly with clients may access client information to better understand their circumstances and past engagement and to deliver a more tailored service.
Searching records for data	Looking through various data sources in order to find information we need. This may involve knowing where to go to search for the data, such as a data inventory or catalogue.	A program officer may look for information about the number of clients accessing a service, or search data.act.gov.au for data on their program target group.
Analysing data to derive information and insights from data	Being able to work with data by organising, examining and evaluating it so that we can discover patterns and form conclusions. We might gather or source the data, review it and apply analytical and logical reasoning techniques to derive information and insights to support our work.	A program officer may use information about rubbish collection to understand where a service offering can be improved, or an executive may consider information about clients accessing a service to understand the issues impacting clients.
Making decisions based on data	Using the insights and knowledge we've uncovered from the analytical process to inform decisions.	An executive may make funding decisions based on data showing the level and intensity of client need across several locations.
Sharing data	Making data available to authorised users – i.e. another agency, organisation or person – in a controlled manner such as through using data sharing agreements.	Data on the water levels within ACT waterways is shared with emergency services to monitor the potential for flash flooding occurring and enable early response.
De-identifying or anonymising data	Making changes to the data to minimise the likelihood of identifying personal information, where unauthorised disclosure might lead to adverse consequences for the individual, agency, organisation or community in general.	A policy officer might make sure no identifying details about clients are provided in a success story included in a report.
Releasing or publishing data	Making data publicly available with no or few restrictions on who may access the data and what they may do with it, including through the ACT Government's Open Data Platform or on an ACT government website.	A report on a community engagement activity might be published on a directorate website.

It is important that all these types of data use, particularly where working with sensitive or personal information, are undertaken in compliance with the legislative framework including the *Information Privacy Act* 2014 and the right to privacy under the *Human Rights Act* 2004.

Leadership

All Executives

All ACTPS staff in leadership roles, including executives who do not have a specific data role attached to their job, have a responsibility to collectively champion a strong data culture across the ACT government. Strengthening and supporting our data culture will enable us to maximise the benefits of trusted and safe data use and sharing to deliver better outcomes for our community. Executives are responsible for ensuring strategic data use to deliver outcomes for the community.

The Director-General may appoint an executive to representative their directorate on the whole of government Data Steering Committee.

Leaders are responsible for building their knowledge and capabilities in data and supporting their staff to value building and using their own data skills and data literacy. All leaders are accountable for data decisions in their respective areas and are responsible for ensuring appropriate data use and sharing by staff, in compliance with relevant policy and legislation.

Chief Digital Officer – whole of Government

The Chief Digital Officer (CDO) works with Executive Data Leads (chief data officers) to improve data practice maturity and support a positive data culture for ACT government. This includes collaboratively developing and updating whole of Government data policies, standards and guidelines.

The CDO works with all executives and the directorate Executive Data Lead to apply the principles in the *ACT Digital Strategy* and the *Data Governance and Management Framework*.

The CDO supports the government to build and maintain community trust in how data is used. The CDO assists directorates to ensure transparency and integrity in the capture and use of data, for example by supporting easier ways for community members to manage their information and give or remove permissions to use their data via the ACT Digital Account.

The CDO is responsible for data security and cyber security policy. When there is a significant data breach or security incident involving personal information, the CDO represents the ACT Government in communicating to the community about the issue and the ACT Government's response. The CDO will work with directorate Executive Data Leads to implement a quick and effective response where required.

Directorate Executive Data Lead (or Chief Data Officer)

Executive Data Leads are accountable for safe and competent data practice across their directorate, championing data use and improving the maturity of the directorate's data practice. Executive Data Leads oversee data management efforts, improve data governance and align data activities with whole of government strategic vision. They proactively encourage data sharing and facilitate the establishment of data sharing agreements. They represent their directorate on whole of government data committees.

An Executive Data Lead will oversee a range of data functions that may include data management, data quality, data governance, data architecture, data science (including analytics), business intelligence and data security. They achieve this through working closely with data custodians, system owners, privacy officers and records officers.

The Executive Data Lead supports data custodians and stewards to ensure good data protections are in place. The Executive Data Lead will ensure their directorate has a data breach response plan setting out how the directorate will contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals. In the event of personal information being lost or subjected to unauthorised access, disclosure or use, the Executive Data Lead works with the data custodian and data steward to apply the response plan and may work with the Chief Digital Officer where appropriate.

Ideally, each directorate will appoint a designated Executive Data Lead or chief data officer to fill this role. However, an alternative is for these responsibilities to be a function of an existing role, such as the Chief Information Officer or even a Director-General or Deputy Director-General.

Agency Security Executive

Agency security executives are delegates of the Director-General or CEO with authority to approve protective security programs for their directorate or agency.

Data Roles

Data Custodians

Data custodians are accountable for governing and overseeing the management of one or more datasets. They may be assigned both internal datasets and datasets that have been externally acquired. Data custodians can authorise the design, capture or generation of data for any purpose, including that it meets business requirements. They also authorise data access, sharing and use where there is a clear public benefit. They ensure processes to capture and handle data, as well as to safely and effectively share data, comply with relevant legislation and policy, including by using the Five Safes data sharing principles.

Data custodians are responsible for establishing data breach plans for their datasets in alignment with the whole of government approach. When there is a data breach or loss, the data custodian implements a quick and effective response, working with the directorate's Executive Data Lead, Director-General or Deputy Director-General as necessary.

A data custodian is not an IT specific role. For example, a data custodian might be an executive who is accountable for delivering a program that generates data on the program's target group or service users.

Data Stewards

Data stewards are responsible for the day-to-day management of one or more datasets, reporting to the data custodian. While they can facilitate data access, sharing and use, authorisation must be provided by the data custodian. Data stewards are the "go-to" expert for the data – they know how the data is captured, maintained and interpreted. They ensure all documentation relating to the data is current and maintain records of access, use, sharing and release. They ensure the data is discoverable through a data register or catalogue. They define the data in a glossary, manage metadata, ensure dataset quality and trust and monitor its use. Data stewards are responsible for protecting the data, while providing information on potential risks and offering regulatory guidance.

Data stewards implement data management practices that uphold safe, secure and trusted use of data, and work with the data custodian to ensure data management is compliant with relevant legislation, policy, standards and guidelines. When there is a data breach or loss, the data steward informs the data custodian and works to implement a quick and effective response.

A data steward may functionally be located within a business or an IT area. For example, a data steward might be a senior manager whose role includes facilitating access to data from a dataset, such as enabling medical staff to access information about patient health needs in order to deliver services.

Both data custodians and data stewards are responsible for:

- understanding and ensuring compliance with ACT Government and directorate strategies, policies and legislation that guide data use;
- making it easier to find, access and use data that benefits the public;
- encouraging and enabling information and data sharing unless there is a legislative requirement not to;
- helping to build public confidence in the safe, secure and trusted use of the data; and
- supporting the publication and release of data through the ACT Government's Open Data Platform.

Summary of directorate-specific data roles and functions

Directorate Executive Data Lead is accountable for

- data sharing arrangements and data governance decisions for all internal and external datasets
- establishing and implementing directorate Data Strategy
- compliance with data policies and practices including whole of government *Data Governance and Management Framework*
- data protections and data breach response plan
- data architecture decisions including data standards for all directorate data systems
- ensuring all directorate datasets are assigned a data custodian and data steward
- championing and fostering a data culture.

Senior executive level and represents the directorate on whole of government data committees.

Data Custodian is accountable for

- data governance and management decisions for internal and external datasets assigned to them
- authorising safe data sharing where there is public benefit to do so
- appointing and overseeing a data steward to manage the day to day operations of the datasets
- implementing and compliance with data strategies, policies and practices and whole of government *Data Governance and Management Framework*

Typically, senior executive or senior directorate level, although their functions may be delegated to the subject matter expert within their branch.

Data Steward is responsible for

- operational data management and decisions for the internal and external datasets that are assigned to them
- documenting and managing dataset register/catalogue, business glossary, master data, metadata and quality specifications
- ensuring the data meets business requirements for all relevant line areas and is *fit for purpose*
- advising and coordinating data sharing to authorised users in accordance with data sharing rules and agreements
- delivering directorate data strategy
- managing any license arrangements for external datasets
- providing a statement of compliance with the directorate data strategy and the *Data Governance and Management Framework* to data custodian, their respective executive and the Executive Data Lead.

Typically, Senior Director or manager level or equivalent, although their functions may be delegated to the subject matter expert within their team.

Other related Roles

This Framework acknowledges the important alignment and support that these data roles provide to other organisational disciplines associated with ensuring data privacy, security, protection and retention.

System Owners

System owners are at an executive or senior executive level and are responsible for management, procurement, modification and enhancement, integration and retirement (life) of a system that hosts one or more datasets. They support access, use, sharing and release of data where required. They have the authority to make binding financial and operational decisions regarding an ICT system, and accept the risks associated with the system, on behalf of the Director-General. They ensure data security and privacy by design is built-in and monitor and resolve technical issues.

System owners work closely with data custodians and data stewards to ensure data is secure in its different states – at rest, in transit or in use. They ensure appropriate records, privacy and security controls and plans according to legislation and policy. When there is a data breach or loss and system failures are involved, the system owner will work with the data steward and data custodian to resolve the issue.

System owners are responsible for ensuring systems allow interoperability[6] and data sharing, including using data standards for commonly collected data elements where possible. A system owner owns an ICT system at the business unit or directorate level. An enterprise system owner owns a whole of government or multi-directorate system.

Business Owners

Business owners orient the design, implementation and improvement of data systems to meet business outcomes and create value for government and the community. Under the ACT Protective Security Policy Framework, business owners are responsible for the security of their information and ICT systems.

For example, a business owner might be a senior executive, Director-General, a program manager, an IT business manager or other role with managerial responsibility for achieving business outcomes.

Privacy Officers

Privacy officers are responsible for the application of the Territory Privacy Principles and the *Information Privacy Act 2014*. They provide advice to data custodians, data stewards and system owners on privacy considerations in the design and implementation of data systems.

Records Officers

Records officers are responsible for assessing datasets to determine application of the *Territory Records Act 2002*. They provide advice to data custodians, data stewards and system owners on the design and implementation of recordkeeping functionality in data systems including that data is the appropriately retained, archived and disposed of when no longer needed.

[6] Data interoperability refers to “the ability of systems and services that create, exchange and consume data to have clear, shared expectations for the contents, context and meaning of that data” (Data Interoperability Standards Consortium, available at <www.datainteroperability.org>)

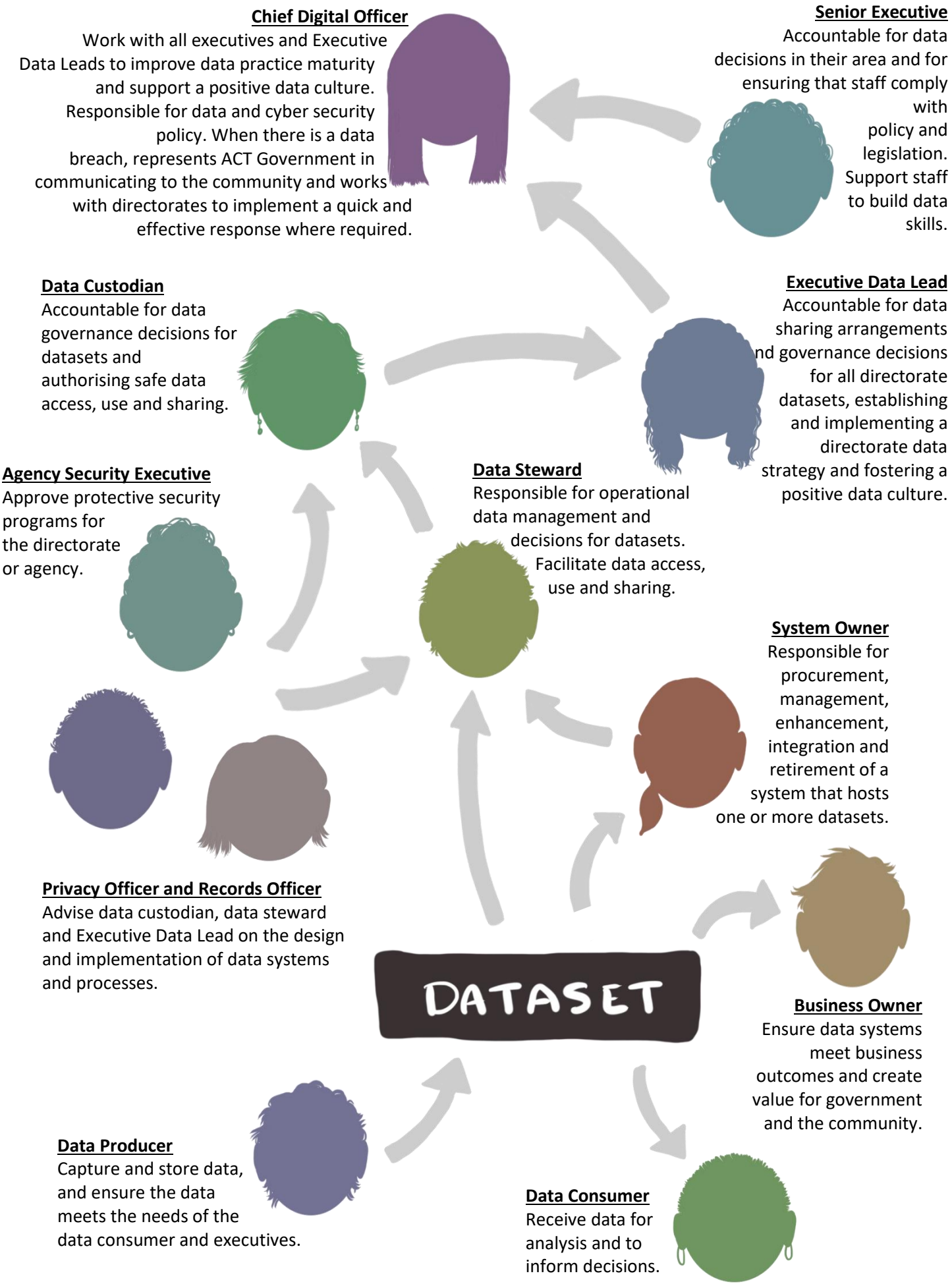


Figure 12 Data roles and functions related to a Dataset

Resources
to identify data roles and responsibilities

A detailed description of the roles of Executive Data Lead, data custodian and data steward is provided in Appendix V.

- Chief Data Officer in Government: A CDO Playbook (Deloitte)
- The Chief Data Officer Playbook (IBM)
- *Data Management Roles and Responsibilities* March 2012 from Forestry, Lands and Natural Resource Operations Ministry in the British Columbia Government – the content worth reviewing are the principles of data custodianship and critical data roles that interact with each other to achieve an integrated data management function.
- Data Governance and Data management skills training
    - Data Management Association International (DAMA) Certified Data Management Professional certification program
    - Coursera
        - Data management https://www.coursera.org/courses?query=data+management
        - Data governance - Introduction to data analytics for business https://www.coursera.org/lecture/data-analytics-business/3-data-governance-k9ePY
    - Swinburne University https://www.swinburne.edu.au/study/find-a-course/information-communication-technologies/data-management/
    - Australian National University Introduction to Data Management, Analysis and Security https://programsandcourses.anu.edu.au/course/COMP2420
- Data literacy and analytics skills –
    - Not only should staff be able to find and understand data, we should be willing, able and capable to use it in new ways to inform decisions.
    -
    - Australian Public Service Commission APSLearn courses: https://www.apsc.gov.au/data-literacy-skills
        - Module 1: Using data in the APS
        - Module 2: Undertaking research
        - Module 3: Using statistics
        - Module 4: Visualising information
        - Module 5: Providing evidence for decision makers
        - Using statistics - 1 day face 2 face program
    - RMIT short courses in data analytics https://online.rmit.edu.au/courses?industry=data_analytics_0

BUILD A CULTURE THAT VALUES DATA AS AN ASSET

1	Establish and promote our shared vision, data principles and values
2	Identify barriers to achieving our data vision and embedding principles in daily practice
3	Identify and foster the desired behaviours of a data driven ACT Government
4	Measure progress towards data vision and reinforce change, and then continuously improve

Data governance and management principles

We are community centred	We are transparent and accountable	We share and use data safely	We are skilled and capable
We make data discoverable	We make data trusted and secure	We value data	We make data open

The ACT Government values data as an asset – second only to our people. All our work to improve data governance and management practice ties back to our culture. Establishing a data culture helps us to be better prepared to work with data in safe and trusted ways. We value data in our culture and practice, and we create public value through data.

Why value data in culture and practice?

The ACT Government is information-rich, with data as the raw material to solve complex policy problems and shape policy priorities, to generate targeted programs, and deliver focused and personalised services to meet community expectations.

We are seeing a shift in ACT Government towards a culture that values data as an asst that can deliver community benefit. Some directorates have established standalone teams that are responsible for managing data and leading organisation-wide data analytics. These teams support functions and practices needed to achieve sustained data and digital transformation. The OCDO has a mix of data policy, data analysts and data engineers to help drive the ACTPS towards data as a cultural norm, while facilitating the management and delivery of data assets at the whole of government level.

Through applying a mix of traditional, contemporary and emerging data analysis methods, such as machine learning and natural language processing, we are shifting from only using historical data to count what was achieved or delivered, to analysing a vast array of structured and unstructured data to help understand why and predict future risks, outcomes and directions. As well as using data for its primary purpose, we can combine and link it with other data to answer more complex and difficult questions, visualise it and tell stories in more detail. In this way, directorate staff can build our capabilities for delivering more timely and responsive services.

What does *valuing data as an asset* mean?

In the public sector, data becomes a valued asset when it is used to deliver community benefit: having been transformed from a raw state to run our day-to-day operations, inform decisions and produce effective and efficient policies, programs and services. We value data as an asset when we:

- consistently use data to improve decision making and create value for the public;
- understand data for its high operational value and refine our organisational structures to better govern and manage data;
- use data for its original purpose and other purposes to benefit the community;
- measure the benefits generated by data;
- build strong foundations to govern staff accountability for managing data;
- define data assets and register them in an inventory or catalogue;
- safely share data with authorised users to create further value and public benefit;
- invest resources to build staff capabilities to realise the inherent value of data;
- release data on the open data platform for use by the community; and
- quantify the financial value of high value data assets (as if on a balance sheet).

All directorate staff, especially those in data roles, have a core mission of capturing, protecting, sharing and using high-quality data assets.

What is culture?

Culture is learned and shared behaviour. It is dynamic and forever changing. Culture influences our everyday experiences. It is in fact *culture* that helps us to shape how we view the world, what we care about, and what we do to build our relationships and engage with others and our surroundings. We transfer our cultural traits – our behaviours and practices – over time and across boundaries and different settings.

As our world changes, we too adopt, adapt and transform our behaviours, beliefs, systems and practices (norms).

What is workplace culture?

Culture exists in our workplaces too: defining our environment and shared values and beliefs, the roles we play, the relationships we have with others and how we communicate, interact and experience our day. It sets the systems, traditions, and attitudes we hold at work. It helps us to identify where we belong and who we can trust and go to for support. We pass on these traits to new people who join our teams.

Great workplace cultures create healthy working environments, attracting talent, driving engagement and satisfaction, and improving our performance.

What is cultural change?

Human societies and cultures are dynamic and forever changing – innovating, learning, growing and building on the past. We tend to shift, reposition and reconstruct our behaviours, practices, and beliefs when we interact with factors around us that influence our perceptions of reality, create knowledge about something that did not exist before, or interact with an existing way of being or thinking.

To make cultural changes in our workplaces requires a disciplined effort to understand the underlying values, beliefs and assumptions that influence how we work and interact with each other every day. It requires flexibility, time, patience and persistence. By understanding the current culture and defining the desired values, behaviours, beliefs, attitudes, systems and practices, directorates can determine the gaps between the current and desired culture, and the leadership, processes, tools, and expertise needed to make and sustain the change.

Culture:

- Is learned and shared behaviour.
- Is transmitted over time and space.
- Helps shape our world view.
- Influences our experiences.
- Is dynamic and forever changing.

In an ACTPS data culture, we:

- Consciously learn, adapt and transform how we work using data.
- Know, trust and use data confidently and consistently in the decisions we make on behalf of the ACT community.
- Protect the safety of individuals in how we use, handle and share data.
- Support and empower our staff to use data.

What is data culture?

A data culture means staff have a collective and shared set of values, attitudes, beliefs and behaviour about using data everyday — we read data, work with data, analyse data and interpret data. We measure outcomes and build on existing knowledge over time.

Employees at all levels recognise the importance of using data and analytical and rigorous approaches to decision-making. We believe data is necessary for our work. We are inquisitive, bold, curious, and tell compelling data stories.

Senior Executives lead by example through championing and using data, rather than only relying on experience or instinct, to shape tactics and strategy. Executives value, demand and invest in data and evidence. They commit to improving staff data literacy, so we too become more capable, reliable and resilient to a changing digital landscape.

Establishing an ACT Government data culture

Building an ACT Government data culture means we make a conscious, consistent and disciplined choice to use data in every decision we make on behalf of the ACT community. Across all directorates, data is consistently *valued as an asset*: we derive value from data by relentlessly using it to deliver public benefit.

When we value our data holdings, we take better advantage of existing and emerging data and digital technologies. We are more productive and better adapt to meet emerging challenges. We collaborate better within and across directorates and with other partners. We harness diversity of views, ideas and tools. We empower our staff to work smarter. Staff in all directorates and at all levels are confident using data and act on trusted insights. Our leaders are committed to using and investing in data and in our capabilities to work with it.

We live in an information and digital age and our community expects us to provide digital services, with tailored and personalised support. In order to do this, we need to adopt and adapt our capabilities, ensuring all staff are data literate and can work with data and data tools. We need a shared set of practices

When we apply the different elements in this framework, we will test the legacy assumptions, practices, as well as the strength and resilience of our organisational culture – but it will also help us change it for the better. **Every day, ask yourself, your teams and your leaders:**

- Are we living our ACT Government data principles; what are our data values?
- Do we care about using data in policy and practice?
- Are we building staff and organisational data capabilities?

and behaviours that help us to deliver value for the community. This is part of being a modern public service, not just part of building a data culture.

In order to use data, we need to know more about the data itself, such as where it is stored and how to access it, who is accountable for the data and what the data is about. Part II of this Framework supports us to make our data discoverable, understood, high quality, safe and secure, enabling us to use and share data to realise its value.

The ACT Government is poised to explore how we can calculate the value of our data holdings, for example by measuring the number of times the data is shared and reused, the information and insights it provides and the decisions that it informs. We recognise that the marginal cost of data is reduced every time it can be reused and that when data stops being accessed and reused, its value decreases.

The following steps can help directorates to build a culture where we value *data as an asset*. Over time, these steps are combined into a comprehensive, strategic, and persistent whole.

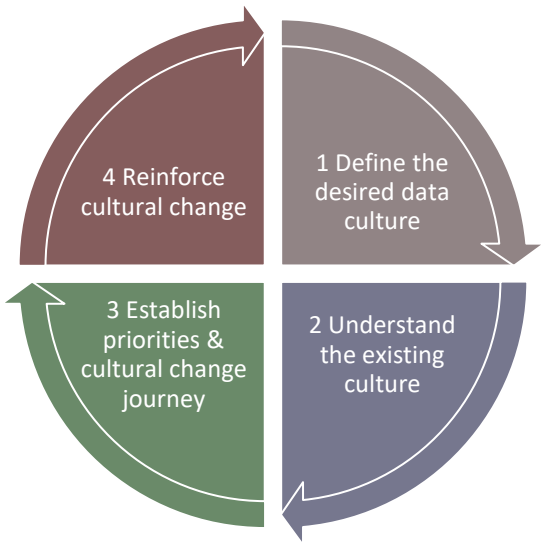


Figure 13 Four Steps to Establish a Data Culture

1. **Define the desired data culture**	Embed our ACT data vision and data governance and management principles • understand how a strong data culture will benefit service users and boost our value proposition to the community; • reflect on the ACT data principles and establish our data values; and • define what makes a strong data-driven culture and the role you and all staff play in creating it.
2. **Understand the existing culture**	Understand how data is currently used within the directorate: • Identify and assess current directorate data culture, its strengths and weaknesses; • determine what needs to change in our directorate culture to improve data use to inform decisions and practice; • identify the gap between the current and future desired culture; • identify directorate data leaders and opportunities; and • prepare stories on why change will support our work and our community.
3. **Establish priorities and cultural change journey**	Establish the priorities that will help us evolve to value data as an asset: • identify change leadership activities and build on cultural strengths; • identify small- and large-scale shifts in behaviour and mindset - identify the behaviours we want to see and behaviours that are no longer desired; • identify our activities and functions that will help us take a more data-driven and digital-first approach in our day to day; • identify data roles and responsibilities across the directorate; and • measure and monitor progress and change.
4. **Reinforce cultural change**	How we communicate, communicate, communicate the change • promote shared vision, data principles and values; • celebrate desired data behaviours, and call out undesirable behaviours • tell our stories and champion a data culture; • recognise soft and technical skills and proven capability; and • reward data forerunners, leaders and change makers.

Our data culture behaviours

By championing and modelling the following behaviours and mindsets, we can foster ACTPS data culture.

Who we are	• We are courageous and forward thinking, inquisitive, bold and curious. • We are nimble, agile, dynamic and collaborative. • We are objective and think critically and creatively. • We learn and innovate and challenge the status quo through new knowledge. • We are open to new ideas and willing to experiment, take risks, fail fast and pivot. • We embrace and celebrate all forms of diversity: gender, sexuality, socio-economic status, culture, age, ability, experience, locational, and divergent thinking (including neurological).
Who are leaders are	• Our leaders value data, use and demand it to inform decisions, prioritise safe sharing of data as an asset and drive good data governance. • Our leaders model desired data behaviours, champion data use, address any fear of exposure or mistakes that prevent data sharing and use, and communicate and reinforce the change. • Our leaders value all staff, invest in data and our data capabilities, and champion diversity. • Our executives empower us to explore, experiment and use data across the public service value stream: policy, programs, service delivery and organisational management.
What we value	• We value the data we hold and use on behalf of our community. • We are custodians of data on behalf of the ACT community. • We value data as a strategic asset to inform decisions and deliver community benefit. • We protect data and use it with care for community benefit. • We build public trust in how we use and reuse data for community benefit. • We believe data is for all staff (not just for a specialist few). • We establish data partnerships with jurisdictions, research institutions, service providers, vendors and private industry to benefit the community.
How we behave around data	• We are data literate: we speak a common data language, we know how to read data, work with data, visualise it and tell compelling stories with data. • We know our responsibilities and obligations when working with data including to proactively protect the privacy and safety of our data holdings, use and sharing. • We know what data we capture, store, use, and manage data as a record. • We work together to change how we think, act and behave with data. • We identify barriers to a data culture and make concerted effort to drive change. • We safely share and release data *by default* (unless there is a demonstrated reason not to). • We know where critical and high-value datasets come from and the processes and methodology by which they were produced. • We make datasets comparable by building in a common data standards. • We build and assess our data maturity.
How we are consistent in our use of data in our work	• We understand what it means to work with data: risks, context, legal and ethical needs. • We use data to innovate and power an efficient, effective and contemporary public service. • We find data from multiple sources, and ensure we use it safely and in trusted ways. • We use data when we plan new policies and identify future trends, forecasts or directions. • We use data when designing and redesigning programs and services. • We take time to understand the data before we use it. • We take a considered, safety-, privacy- and risk-based approach to working with data. • We are transparent about the limitations of any data and the impact this may have on the insights we gain from it to inform decisions. • We use data to track our outputs (what we create), monitor performance (how we are going) and measure our outcomes and impact (are we making a difference). • When we contract an external provider to collect data on our behalf, for example to deliver a program or service, we require the original data as part of the deliverable under the contract.

Resources

to support work to establish a culture that values data

- In 2018 the Australian Government commissioned the Independent Review of the Australian Public Service, led by Chair David Thodey AO, to help ensure the public service remains fit-for-purpose in the decades to come. The 40 Australian Public Service Review recommendations and supporting APS reform agenda strive for a stronger, contemporary public service culture and purpose, systems, tools and processes. Accelerating the adoption of data and digital technologies is at the forefront of this APS reform for data-driven and digitally enabled government.
    - https://pmc.gov.au/news-centre/government/governments-aps-reform-agenda-world-class-australian-public-service
    - To better harness the power of data, the following data and digital ambitions highlight key aspects of a data and digital culture in government to solve complex policy problems and enable the APS and the Government to work together seamlessly.
    - By 2030 a data-driven and digitally enabled APS will:
        - deliver personalised, integrated and proactive services to people and businesses — whether online, in person or on the telephone;
        - use data, advanced analytics and emerging technologies to achieve the best outcomes for people and businesses;
        - drive productivity and efficiency in government services;
        - collaborate and integrate seamlessly across departments, agencies and different levels of government, including ensuring that information only needs to be provided to government once;
        - provide pervasive digital leadership and talent across all agencies and levels, and have strong whole-of-government data and digital functions; and
        - have access to global best-practice digital learning and development programs to incubate new talent and next generation skills.
- Example – Good practice in creating a data culture
    - Canada's Open Government Portal provides access to government data and information and demonstrates Canada's international commitment to transparency and open government. The site contains targeted search capabilities and datasets compiled by over 43 departments and agencies, covering a broad range of topics, from housing, to health and environmental data. Users can explore local census or crime statistics, immigration and air quality data, coast-to-coast-to-coast mapping data, and much more.
    - As one of its key open data initiatives in 2014, the Government of Canada supported Canadian Open Data Experience (CODE) as a founding partner. CODE – Canada's first national open data hackathon – gave Canadian post-secondary students, entrepreneurs and innovators the experience required to turn federal government data from Canada's Open Government Portal into user-friendly applications for the benefit of Canadians. CODE 2015 was the second annual edition in the CODE event series. CODE is an example of how the Government of Canada is promoting and supporting open data. As a result of this work, more than 200,000 datasets from 43 federal departments and agencies are currently available via open.canada.ca under a common Open Government Licence – and new datasets are being released on a regular basis.
- In 2014, the OECD presented a Recommendation on Digital Government Strategies aimed at bringing governments closer to citizens and businesses. This recommendation included the following points on creating a data culture:
    - Better exploit digital technologies and data analysis to understand societal needs;

    - Embed the use of data throughout the policy cycle;
    - Put in place governance arrangements to ensure responsible and coherent use of data that benefits citizens and strengthens public trust; and
    - Develop a culture of data analysis and use within the public sector that helps predicting new needs and trends and understanding how to improve existing processes and dynamics.
- Data Culture advice from Gartner and McKinsey
    - https://www.gartner.com/smarterwithgartner/the-key-to-establishing-a-data-driven-culture/
    - https://www.gartner.com/smarterwithgartner/create-a-data-driven-culture-by-influencing-3-areas/
    - https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/why-data-culture-matters

PART II – A MANAGED AND MATURE DATA PRACTICE

This section provides the foundational steps to build our data maturity where staff work with data to drive trust and improve community outcomes.

- ☐ MAKE DATA DISCOVERABLE
- ☐ MAKE DATA UNDERSTOOD
- ☐ IMPROVE DATA SHARING
- ☐ ENSURE QUALITY DATA
- ☐ MAKE DATA SAFE AND SECURE

MAKE DATA DISCOVERABLE

1	Set up data roles, responsibilities and governance.
2	Identify directorate datasets.
3	Identify, appoint and train data custodians and data stewards.
4	Register datasets in a data catalogue.

Data governance and management principles

We are community centred	**We are transparent and accountable**	We share and use data safely	We are skilled and capable
We make data discoverable	We make data trusted and secure	We value data	We make data open

To effectively govern and manage our data, we need to be able to find it and understand what kind of data it is. The next two sections of this Framework deal with how we make data 'discoverable' and 'understood'.

At a very simple level, to **make data discoverable** means to make the data asset visible in a safe and secure way – enabling staff across directorates and government to gain a high-level understanding of the data held by directorates and promoting the greatest possible return on its value through its widest possible use. Data discovery (sometimes called indexing) means listing datasets on a searchable database so that staff can find them. The dataset itself does not need to be accessed this stage.

To make data discoverable in a way that is useful to our work, the listing should include a minimum set of information about the data including: the dataset name, where it is held, what it is about and who the key contacts are. Further information about *how* we make data discoverable is provided below.

Why make data discoverable?

By making data more discoverable, the ACTPS can enable data users to use and build upon existing data, instead of recreating it, to solve common problems across traditional policy or portfolio boundaries and foster innovation. By reusing data, the ACTPS can verify and validate policy, program or service outcomes, reduce duplicated effort, uncover new findings from existing data, and integrate datasets for new analysis.

To access and use data, we need visibility of our data assets. Often, staff do not know what data exists, or where to go to find and access the data we need. Finding data can also be like looking for a needle in a haystack. With no consistent and easy way of searching for ACT Government data holdings staff may spend time looking for data in the wrong places and not finding it, duplicate effort or (worse still) not use data in their work at all.

For our staff to deliver data-driven decisions, we need to put data in their hands. Data needs to move out from hidden repositories and from a handful of data experts. Data needs to be democratised.

Making data discoverable supports staff to do their work more effectively. As data users, we can easily find the data we need when we need it, know how to access it, know who to contact for more information about the data, check the suitability of the dataset for their needs and understand what we can and can't do with the data, such as sharing it. Data custodians can better describe their data holdings, share information about it such as through data registries or catalogues, provide advice to data users and reduce risks to data through inappropriate access and use.

By taking a disciplined approach to making data discoverable by users, data custodians can enable quick and efficient searches, greater understanding and visibility of the ACTPS data landscape, maximise the value of data holdings by making best use (and safe sharing) of existing data, and drive data-informed policies and practice.

How do we make data discoverable?

There are four steps to make each directorate's data discoverable:

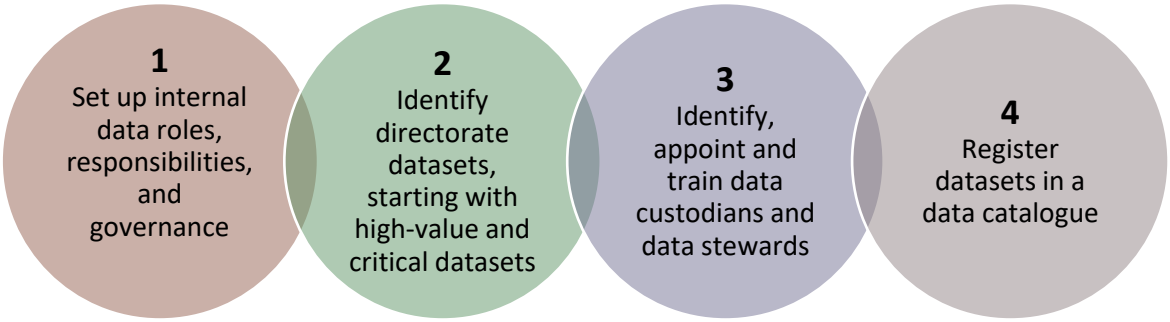


Figure 14 Four Steps to Making Data Discoverable

First, set up governance arrangements for our data, including identifying relevant roles and responsibilities. Data custodians, data stewards, Executive Data Leads and data governance groups are accountable for overseeing data governance, management and use. They ensure that appropriate steps are taken to make data discoverable and that data is captured, protected, shared and used appropriately.

Second, identify the datasets that are held by each directorate. These might be in different formats and in different systems, from excel spreadsheets to ICT systems like the Community Services Directorate's Child and Youth Reporting and Information System (CYRIS) or ACT Digital. Start with the most critical datasets before attempting to list all datasets. Some directorates will have a significant number of datasets and it is more important that critical datasets are discoverable earlier than those datasets that may no longer be active or essential.

Third, identify, appoint and train data custodians (accountable) and data stewards (responsible) for those datasets. Data custodians and data stewards make data discoverable by describing the dataset (such as the name, location) and are the key contact point for data users seeking to access and use the datasets. Refer to the section of this Framework on data roles and responsibilities, for further information.

Fourth, data custodians or data stewards will register or list datasets somewhere that is searchable. Ideally, all datasets across ACT Government will be searchable through a centrally accessible hub or repository, such as an ACT data catalogue or other form of data register. The data itself may not be stored in a central location, but the information *about* the data should be centrally accessible. We should be able to identify that a dataset exists, even if we are unable to access the data itself. This will help to resolve barriers to accessing and using the data. A register of data users may be developed to record and monitor access and use, where required and depending on the data sharing requirements and arrangements.

On its own, a dataset name is not enough for staff to access the data or establish whether the data will support their work. We also need to know the following:

- Where is the dataset stored? (e.g. the system and directorate where the data is held)
- Who are the key contacts for the dataset? (e.g. the data custodian and data steward responsible for authorising and facilitating access to the dataset)
- What is the purpose of the dataset?
- Are there any restrictions on accessing, using or sharing the dataset?

Additional information may also be included to improve discoverability, such as how the data was captured and where it originates, whether it was purchased, who can access it and a link to the data itself.

Resources
to support work to make data discoverable

Some directorates have existing dataset registers or data catalogues (some tools enable automation of data discoverability). Directorates also have registers for business systems, software licences, or risk and security plans that may include details about the data holdings. The ACT is in the process of establishing a whole of government data catalogue to provide a centrally searchable repository where datasets can be located.

Executive Data Leads, data custodians and data stewards should seek updates on ongoing work and advise data users in their directorate as new data discoverability tools become available.

Steps to enablement	**Make Data Discoverable**
Objectives	• Know what datasets are held by Directorates and who manages them
Outcome	• Know what datasets we hold (data register on a central location) • Search and find the datasets we hold (data register on a central location) • Know who is looking after the dataset (data roles and responsibilities)
For Data Users	• Can easily find the data that they need and can contact a Data Custodian for more information.
For Data Custodians and Data Stewards	• Can make dataset discoverable to the ACTPS • Can share information on the data and provide advice to Data Users.
Example activities:	• Identify Directorate datasets, starting with high-value and business critical datasets • Identify and appoint Data Custodians • Identify and appoint Data Stewards • List datasets within Agency / Directorate • Represent Directorate at ACT Government groups • Train Data Custodians and Data Stewards in data governance and management • Register datasets in the ACT data catalogue • Establish internal governance arrangement including Executive Data Lead • Represent Directorate at ACT Data Management Committee
Example resources and tools in congruent with DAMA DMBOK and Office of the National Data Commissioner Need to define who is responsible for 1) design the product 2) implement the product in practice 3) maintain and improve the product	• **Data Register/Data Catalogue** located on a central repository or hub incl Data Custodian, Data Steward, contact details, data type, dataset purpose, system and storage location, disclosure, sharing rules, open data • **Data Governance and Management roles**: Define Data Custodianship and Data Stewardship roles descriptions, develop data custodianship and stewardship training and on the job learning opportunities, and establish a community of practice specifically for data custodians and data stewards • **Data Governance Mechanisms** for ACT government and directorates

MAKE DATA UNDERSTOOD

1	Prepare business glossary for the dataset.
2	Prepare data dictionary for the dataset.
3	Identify primary use of the data.
4	Outline data sharing rules for the dataset.

Data governance and management principles

We are community centred	**We are transparent and accountable**	We share and use data safely	We are skilled and capable
We make data discoverable	**We make data trusted and secure**	**We value data**	We make data open

At a basic level, **making data understood** means describing the data well-enough so that data users can know how, when and why the data was captured (origin), why it is used (usage) and what it is made up of (format). This can also include information about whether the data can it be shared and accessed, and if it can be used for purposes other than its primary purpose.

To make data discoverable, data custodians and data stewards need to define the key characteristics (**metadata**) of the data in meaningful terms. This includes data that was acquired from external sources. Data users, data systems and applications use metadata to understand the meaning of the data and information. Metadata exists in many sources. Data glossaries can be used to understand business-facing definitions about the data. A data dictionary can be used to learn the technical definitions of the data. Data models document, define, organise, and show potential data users how the data structures within the database, architecture, application, or platform are connected, stored, accessed, and processed.

By describing the data and communicating it to potential users, we can make data more available, accessible and understandable. This kind of "semantic" data layering can provide a common language to enable the use and reuse of data to inform decisions. Making data understood builds on the work we do to make data discoverable.

Making data understood reduces the risk of data being mis-understood, mis-interpreted and mis-used. Often, it is not about whether staff have the right skills and capabilities to work with or analyse data, but about how we make specific datasets easier to comprehend and use.

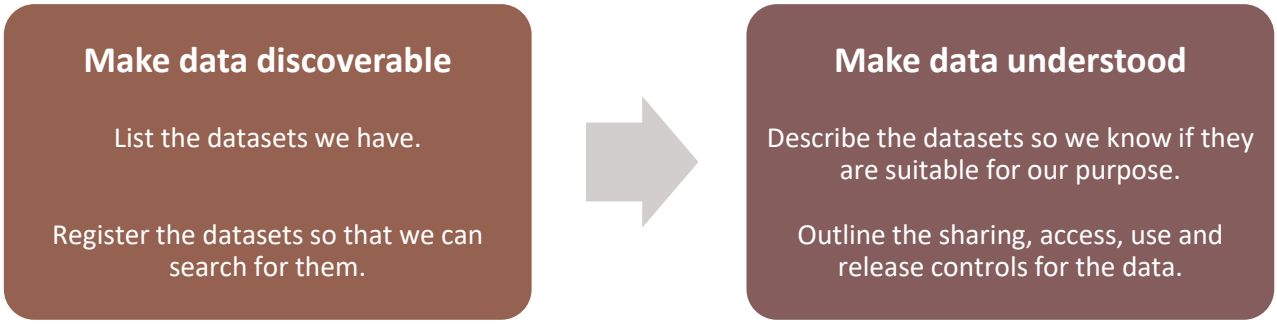


Figure 15 From Making Data Discoverable to Making Data Understood

Why make data understood?

Data needs to be described so we know what data we have, what the data is about, understand its context and purpose, and can find it easily. This descriptive data is called metadata. By including metadata, for example in a data glossary or data dictionary, users can recognise whether the data is suitable for their purpose and how to use it. Without this information, we cannot successfully manage our data and we cannot make the most of our data assets to deliver better outcomes for our community.

Making our data understood also means we can better manage the safety and security of our data. We can quickly identify data that is private or sensitive and provide clear information about the data sharing, controls and data release requirements for every dataset we hold. This information will help data users safely access, share and use data, and will help data custodians and data stewards to respond better to data breaches.

We make data understood so that we can better use, govern, manage and share our data. We can improve our ability to easily find data, understand its purpose, and use and share it by ensuring we apply common data design and standardisation processes within directorates and across government. These include using consistent metadata structures support efficient and robust cross-analysis of data from different areas. Applying common ways (standards) for data labels, type and value domains can help reduce inefficient and costly processes.

Metadata

Simply put, metadata is 'data about data'. Metadata contributes to our ability to govern and manage our data through better understanding of our data and the systems, people and processes that create, maintain and use the data.[7] This supports us to:

- identify, authenticate and contextualise data and information;
- conduct quality assessment and manage databases; and
- control, manage, find, understand and preserve information over time.

There are many types of data or information that can be called metadata. It is possible to create a *minimum* metadata set to ensure datasets consistently record essential metadata elements, to support interoperability between systems and processes and to facilitate better data use. Some examples of metadata that might be included in a minimum metadata set are provided below.[8]

- Title
- Author (data custodian, data steward)
- Registration number or other unique identifiers
- Date created or received
- Subject matter and keywords
- Format
- Extent (geographical area covered by the data)
- Data quality
- History of use.

Metadata is like…

Consider a can of food in the supermarket. Without its label the can is just a silver can like any other. The label gives us all the information about the contents including a description of the product, instructions for cooking and suggested additional ingredients. We use the label to choose whether to purchase the can and how to consume it.

The National Archives of Australia advise: "Metadata standards ensure metadata is consistent useful and understood over time. Establishing a minimum metadata set in your agency will also help you understand your user and business needs. This will help prioritise metadata for remediation and ensure that compliance with metadata standards is not an after-thought in developing new systems and processes."

For more information on metadata, view this video produced by the Intergovernmental Committee on Surveying and Mapping Metadata Working Group.

Master and Reference Data

Master and Reference Data can help ensure that data is defined consistently, and where possible standardised across the directorate and whole of government. They assist with connecting common and related data in different records, files, tables and other storage formats. They help determine records for lookup, cleaning, linking and matching. They can be used to represent shared data across Directorates and, where possible, across the ACT Government and other jurisdictions. Directorates may have an agreed set of master data and reference data models for use to better manage the data standards for the directorate.

Master data is data that is agreed and shared across the directorate, for instance the name and address of an ACT resident, customers, and employees. Reference data is a subset of master data to classify or categorise data within the dataset based on a permissible set of codes or values. Examples of reference data include geographical lists like suburb names and codes, state names and codes, country codes, industry classifications, and gender. The Australian Bureau of Statistics provides a set of nationally consistent standards for statistical data such as the Australian Statistical Geographical Statistical Areas.

[7] DAMA (2017), pp417-418

[8] National Archives of Australia, *How Metadata is Used*, available at <https://www.naa.gov.au/information-management/describe-information/metadata>

Master data management and fostering common data standards (data and metadata fields) can enable directorates to identify, integrate, and cross-reference data from across the ACT Government. We can better match records and datasets, and use business rules to clean, remove duplicates, match and merge records. By improving enterprise data and information architecture and master data, reference data and metadata management processes, directorates can establish common, consistent and authoritative data standards and information records at the outset of system procurement and solutions design.

How do we make data understood?

There are four steps to make each directorate's data understood, once we have made our data discoverable. Data Custodians and Data Stewards can follow these steps for every dataset they are accountable for – starting with high-value and active datasets.

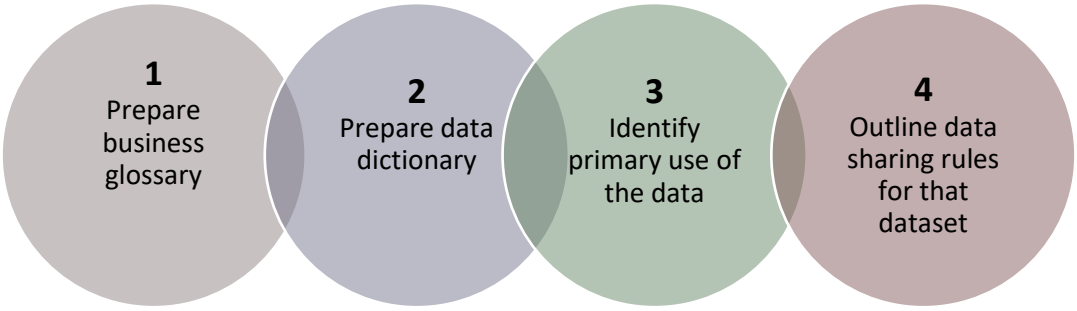


Figure 16 Four Steps to Making Data Understood

First, prepare a business glossary of items relating to the dataset. A business glossary defines the data using ordinary operational or business language so that it can be easily understood by staff and users. It does not define terms in a data or ICT system sense. For example, what do we mean by a customer, a regulation, a school or an appointment? In one directorate, staff may use the term "customer" to represent the individual receiving the service, while another directorate may use the term "client", "patient" or "student". The scope of the glossary should be agency or directorate-wide where possible to ensure consistency in how items are defined and interpreted. Data custodians and data stewards will need to also identify which items are defined and which items or terms still need to be defined.

Second, prepare a data dictionary. There should be one data dictionary for each dataset or database. A data dictionary should include technical metadata for the dataset, including descriptions and details involved in storing the data. It should include details such as data type, permissible length and permissible domains (values). While tools are available to determine many of these technical details from scanning and profiling the data itself, there is still a need for subject matter experts to define and describe the data elements and business rules associated with the data. The metadata in the data dictionary helps data analysts and other users understand how to join, query, interpret and report on the data.

Third, clearly identify and define the primary use of the data (why it was captured). Identify requirements such as informed consent and whether this was received during data capture or acquisition. This is useful to note in the metadata, as it enables data custodians and potential data users the ability to define and assess the potential for acceptable secondary uses of the data.

Fourth, to support data discoverability, data custodians are responsible for helping potential data users to know whether the data can be accessed and shared. As the ACT Government moves to enable safe and trusted sharing of data, the metadata for the dataset should outline the high-level controls and/or restrictions for accessing, sharing, using or releasing of the data. This information is known as the data sharing rules. See the 'Improve Data Sharing' section of the Framework for further activities to enable and manage authorised sharing and access to data.

Resources
to support work to make data understood

The ACT is in the process of developing a whole of government data catalogue, which will provide a centrally searchable hub where datasets can be registered. Executive Data Leads, data custodians and data stewards should seek updates on ongoing work and advise data users in their directorate as new tools become available to support making data understood.

Steps to enablement	Make Data Understood
Objectives	• Understand what datasets can and cant be used for
Outcome	• What is the purpose of the dataset (register, glossary, metadata) • Know what the data means (metadata) • Know who can access them (data sharing)
For Data Users	• Can check suitability of the dataset to their needs using the data definitions • Can understand the sharing rules.
For Data Custodians and Data Stewards	• Can reduce risk of misrepresentation of results from analysis by Data Users • Can help ameliorate risks of data breaches.
Example activities:	• Prepare dataset metadata and business glossaries • Outline data sharing and data release requirements • Develop data models
Example resources and tools in congruent with DAMA DMBOK and Office of the National Data Commissioner Need to define who is responsible for 1) design the product 2) implement the product 3) maintain and improve the product	• **Dataset / Business Glossary**, logical data model, physical data model, common reference/master dataset model • **Metadata** standard + geographic metadata standards, how to write up meta data and list of metadata types • **Safe Data sharing and access** support including ACT Government data sharing arrangements, privacy legislation and processes, data classifications, guidelines for data incident (breaches) of information security/confidentiality • Open Data Support

Existing metadata standards are already being used by directorates. These include:

- The ACT Open Data website, which allows the public to search for ACT Government open data using the metadata fields populated by directorates when uploading data.
- The ACT Government's Open Data Geospatial Catalogue enables this for geospatial data on ACTmapi
- The Australian Institute of Health and Welfare's Metadata Online Registry (METeOR)
- The AGLS Metadata Standard issued by Standards Australia as AS5044: 2010 has been mandated for use by Australian government agencies. The Digital Service Standard also requires the application of AGLS metadata to online resources.
- See also the advice on metadata by the Metadata Working Group under the Intergovernmental Committee on Surveying and Mapping and located on the EMSINA website
- The ACT Government's Human Services Cluster established the Common Dataset for Human Services to guide the capture and use of data across the human service in the ACT
- The ANZLIC – the Spatial Information Council has developed the ANZLIC metadata profile to facilitate the interoperability within and between Australian and New Zealand agencies and jurisdictions and is based on the ISO 19115 international standard. The ISO 19115 schema is the

preferred international standard for spatial resources. It can be generated by the following open-source tools: ArcGIS | ANZMet Lite | GeoNetwork | Other software and tools

- Also see the ANZ Metadata Profile of the ISO 19115-1:2017 for datasets https://www.icsm.gov.au/sites/default/files/Poster%20-%20Best%20Practice%20for%20Datasets%20Metadata%20v1.pdf
- The National Archives of Australia publishes the Australian Government Recordkeeping Metadata Standard (AGRkMS) as well as detailed resource on Metadata for interoperability. The ACT Territory Records Office has endorsed the AGRkMS for use in the ACTPS.

IMPROVE DATA SHARING

1	Foster a data sharing culture
2	Understand the risks, barriers and challenges to data sharing and release
3	Understand the legislative and policy frameworks that govern data sharing
4	Establish clear and consistent governance and management practice to enable safe data sharing, including by adopting the Five Safes data sharing principles
5	Improve open data by safely releasing more ACT Government datasets on data.act.gov.au

Data governance and management principles

We are community centred	We are transparent and accountable	We share and use data safely	We are skilled and capable
We make data discoverable	We make data trusted and secure	We value data	We make data open

The ACT Government is committed to safely sharing, reusing and releasing public sector data to benefit the community, while remaining accountable and transparent. To achieve this, we foster a culture that promotes safe and trusted data sharing in accordance with relevant legislation and policy.

This section of the Framework provides guidance on improving the processes we use to share data safely, balancing the public benefits of data sharing with managing the risks. This guide helps build a common model for data sharing across ACT Government, supported by consistent, shared data management practices.

Data Sharing

Put simply, data sharing means making information or data "available to another agency, organisation or person under agreed conditions."[9] In the ACT Government context, this means we might share data within and between directorates, with other jurisdictions and with non-government organisations providing services on behalf of the government. It can occur on a systematic or ad hoc basis, but always under agreed conditions.

We share data for a range of purposes, including to:

- plan, design and deliver government policies and programs based on the best available insights;
- conduct monitoring and evaluations or support compliance and reporting measures; and
- conduct and support targeted research to benefit the lives and wellbeing of the ACT community.

. When and who we can share information and data with depends on the context:

- What kind of data or information is it?
    - de-identified data (where personal information has been removed)
    - identifiable data (information that is able to identify an individual, organisation or other entity)
- What are the privacy, security, freedom of information and records management considerations?
- What does the relevant legislation and policy allow and enable us to share?

As data users, we have a responsibility to safely manage the data we hold and use on behalf of the community and those who provide the data to us. The ACT community expects us to use, handle and share their data in a safe, transparent and accountable way in line with requirements in privacy and portfolio legislation. We are responsible for ensuring that data is used and shared in a way that maximises the benefit to the community. We are also responsible for ensuring appropriate protections are in place to minimise the likelihood of breaches of privacy or security, such as sharing personal information when not permitted or required.

Data sharing is different to **open data** or **data release**. When we share data, we are clear about who it is shared with and why, and the specific conditions, controls, and safeguards under which it is shared. Open data is publicly available data that can be freely used, reused and redistributed by anyone. The ACT provides open data to the community to support economic growth, improve service delivery and achieve policy impact. The diagram identifies the spectrum of data sharing from closed to open.

[9] Office of the National Data Commissioner (2019), *Best Practice Guide to Applying Data Sharing Principles*, available from <https://www.pmc.gov.au/resource-centre/public-data/data-sharing-principles>

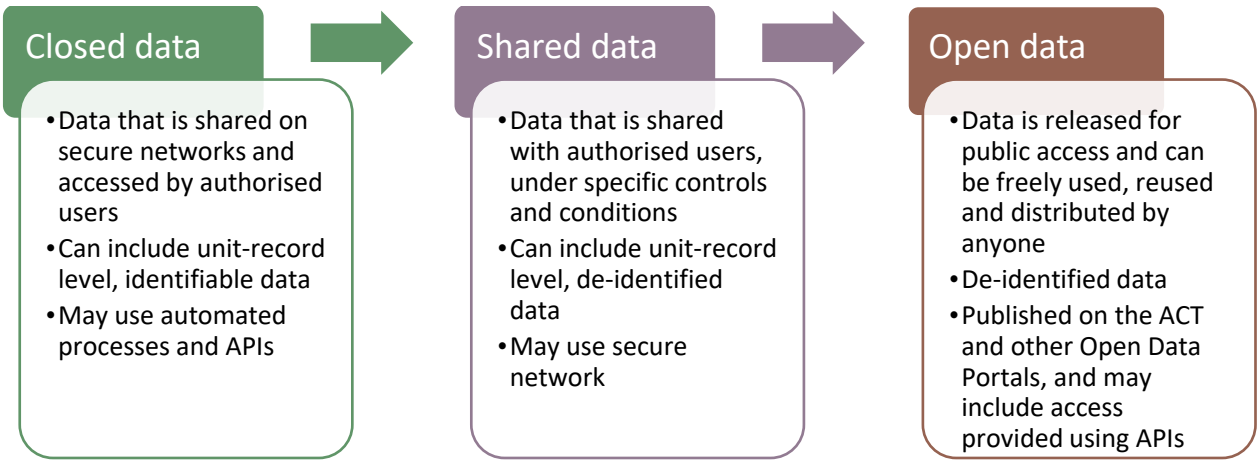


Figure 17 Data Sharing Spectrum - from closed to open

Why improve data sharing?

By improving information and data sharing alongside improvements to data governance, we can benefit the Canberra community through facilitating:

- greater community wellbeing through better services, planning, policy and research;
- improved trust in government use and protection of data and information;
- streamlined and efficient public services, delivered in more convenient and tailored ways;
- improved identification and timely services for Canberrans with diverse and complex needs; and
- increased economic activity, competition, growth and productivity.

The value of the data that we capture, protect, share and use on behalf of the community is maximised through use, reuse and sharing so that it can be used to inform and improve decision-making.

Sharing data between different parts of the ACT Government can help to provide a more comprehensive picture of issues impacting vulnerable Canberrans, enabling faster and more effective responses and significantly enhancing efforts to improve community safety. In the past, the ACT has witnessed tragic consequences from failures in information sharing. This includes family violence cases where multiple services knew of isolated incidents but lacked mechanisms to draw information together from disparate systems or share information early and effectively, limiting services' ability to make fully informed decisions.

It is important to ensure that information is shared safely. The 'Context' section of this Framework identifies risks in relation to data sharing, including that wrongful information sharing can cause harm to the community.

What are the barriers and challenges to sharing data?

Risk averse culture

- Staff report a lack of understanding about when information and data can be shared, for what purposes, and with whom. Often a cautious view is taken of the risks associated with sharing. There are rarely any direct consequences for withholding personal information, while inappropriate disclosure or capture can have major repercussions. This can result in information not being shared, even when there is a legal basis or community expectation to do so; meaning that individual discretion trumps best practice.
- Unknown or unclear community expectations, together with the fear of undermining trust, contributes to a risk averse approach and a lack of information and data sharing.
- As the potential of data and digital technologies has enabled information sharing, community expectations have changed. It is important that the legislative environment align with community expectations around government services.

Legislation

- Data sharing and release is governed by the *Information Privacy Act 2014* (ACT) and at times other portfolio legislation that regulates how we obtain, use and disclosure personal information, and that may prohibit sharing information (including information about individuals) unless authorised to do so.
- The *Information Privacy Act 2014* (ACT) set out the obligations for data custodians to appropriately manage personal information in accordance with the 13 Territory Privacy Principles (TPPs) set out in the Act. More on this is provided in section 11 of this Framework: 'Make Data Safe and Secure'.
- The many different ACT laws that touch on information sharing can make the legislative framework around data sharing complex and unwieldly for individuals to understand. Additionally, viewing legislation or parts of legislation in isolation from the broader legislative framework carries risks for information sharers.

Governance and policies

- Inconsistent governance, policies and guidelines across the ACT prevent staff from confidently making decisions to share information and data. The roles and responsibilities of data custodians and data stewards are unclear and often inconsistent, hampering their ability to confidently make decisions about sharing information and data with users and releasing open data to the public.
- Lack of clarity or understanding by stakeholders of the provisions relating to data sharing, how that data can be used within ACT Government and/or outside of the ACT Government, and whether it can be released under Freedom of Information may within data sharing agreements, contracts or memorandum of understanding.

Digital infrastructure

- The ACT Government has over 2000 systems that manage data and information. Of these, over 200 are considered government and business critical. Many of the remainder are legacy systems that hamper safe sharing because there is no mechanism for system to system interfaces. This means that when data is shared, it is mostly manually extracted, cleansed and shared through outdated and unsecure mechanisms. This limitation contributes to risk averse approaches to sharing.

Types of Data About Us: Open Data Institute Study

A key challenge in sharing data continues to revolve around the issue of collecting and using *data about people*, and the risks and concerns associated with sharing it. During 2019, the Open Data Institute (ODI) conducted research on data rights and ownership, and sought to uncover the UK public's knowledge and understanding of data protection and control. The ODI found that *data about us* comes in many different forms and that people "generally feel positive about the benefits brought by the internet and being more connected, but want **greater honesty and transparency**, **agency and control**, **rights and responsibility**, **context and fairness**, and **compliance and enforceability** over how data about them is used. Ultimately, they want to know that where data is concerned, they will be treated as people, not as robots."

The ODI's graphic tool below helps describes the different types of *data about us*:

personal data; **sensitive** data; **behavioural** data and **societal** data.

Using this graphic, we can see that data as not being the same – "data can be an identifier; can be more sensitive than other types of data; can provide or create insights; or it can be used to make decisions that don't just affect us as individuals but can affect and improve society as a whole."

The graphic tool can be used to help people to become more aware of the kind of data about themselves they are being asked to share, what data they must share and why, and what data they would prefer not to share. This can further help people better understand what they are being asked to consent to and can assist with improving education. As a result, people can more clearly articulate when they are happy to share and why, as well what communication, transparency and engagement they expect from government and organisations about this.

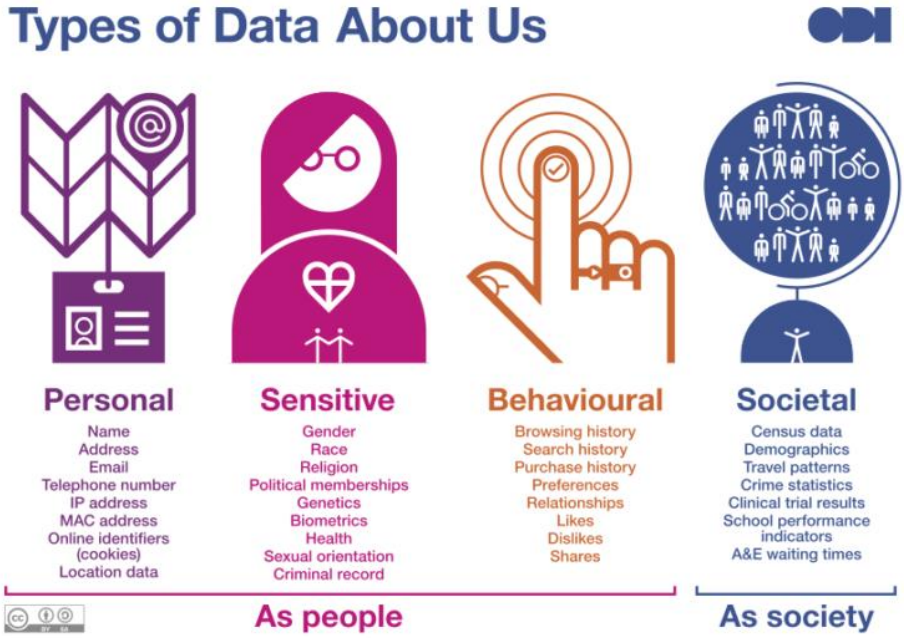


Figure 18 Types of Data About Us
This graphic from the ODI is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

The ACT Government espouses the importance of designing privacy along the entire data lifecycle and as such proposes the need to build in consent-based data collections. Here consent is defined as ensuring individuals' choice and control over how their data is used and take responsibility for ensuring the consent is informed.

Who is responsible for sharing data?

We all have a responsibility to share information and data *by default*, except where not authorised by legislation. Fostering a data culture within and across directorates supports staff to understand the value of sharing and reusing data.

This relies on executive leaders to drive change and for all of us to be better aware of our roles and responsibilities when working with data. in a data sharing culture, leaders foster growth and development in staff knowledge, attitudes and practices around data sharing and use.

ACT Government staff with specific data roles, such as data custodians and Executive Data Leads, are accountable and responsible for leading this change within their directorates:

- fostering and enabling pathways and an environment conducive to data sharing;
- demonstrating the value of sharing data for public good; and
- supporting staff to build their knowledge and understanding of legislation and policy while ensuring privacy and security continue to be protected.

How do we share data safely?

There is a fundamental need to balance the value and risk of data sharing activities, to protect our community and to build community trust in government. The potential risks associated with sharing data are often themed around misuse of data and breaches of privacy.

The ACT Government has adopted the **Five Safes** as a framework to support safe data sharing, building on the Australian Office of the National Data Commissioner (ONDC) adaptation of the Five Safes for its Data Sharing Principles in its *Best Practice Guide to Appling Data Sharing Principles* as the Data Sharing Principles.[10] These principles can provide a "privacy and security by design" approach to help the ACT Government to share data safely while balancing public benefits with risks.

1. PROJECT	• Data is shared for an appropriate purpose that delivers a public benefit. This principle assures data is being shared for the right reasons and outcomes, is legally valid and that there are no ethical or consent concerns. • *How is the data being used? Who benefits?*
2. PEOPLE	• The user has the appropriate authority to access the data. This principle guides thinking about what types of people should have access (skills, experience, and qualifications). • *Who is using the data?*
3. SETTING	• The environment in which the data is shared minimises the risk of unauthorised use or disclosure. This principle considers if data is accessed through a secure lab or some other environment and what controls to put in place. • *Where is the data being used?*
4. DATA	• Appropriate and proportionate protections are applied to the data. This principle considers what data treatments might be needed, particularly to avoid disclosure of sensitive information, e.g. aggregate data fields that would then make it possible to share data. • *Are appropriate protections in place?*
5. OUTPUT	• The output from the data sharing arrangement is appropriately safeguarded before any further sharing or release. • *How are the results of the project used?*

[10] ONDC 2019, https://www.datacommissioner.gov.au/sites/default/files/2019-08/data-sharing-principles-best-practice-guide-15-mar-2019.pdf

Typical data sharing risks and mitigations are discussed below, grouped around the Five Safes principles to better understand how good data governance and management practice can help to lessen these risks while balancing privacy, disclosure, security and other obligations.

Projects – risk where the data is used inappropriately, unethically or illegally; potentially causing harm	
Risk	Risk of shared data being misused, causing harm and loss of community trust in government. Risk of data being shared for a particular purpose but then subsequently used for a secondary purpose that was not part of the initial arrangement or agreement.
Mitigation	Data custodians must assess the intended purpose(s) of the data sharing including whether it is in the public interest (e.g. is the data use to deliver services, to support the design, implementation and evaluation public policy or programs, or to conduct a research activity targeting a public benefit?). The data custodian must check: • whether the project is required to be authorised under legislation; • whether the project requires ethics approval or consent from the data provider; • how the data will be protected from risk of disclosure; • that data can only be accessed and used by an approved user; and • whether authorisation is needed for a secondary use of the data.

People – risk where the data user does not have the knowledge, skills and motivations to ensure safe use and treatment of the shared data	
Risk	Risk of data breach, misuse of data or misinterpretations and inaccurate analytical findings where data users are not appropriately skilled or are unaware of their responsibilities.
Mitigation	Data custodians should ensure that only authorised users with appropriate training access the shared data. Data custodians should ensure that data users understand the expectations and limitations of using the data prior to accessing, storing and working with it and demonstrate appropriate knowledge, skills and experience to work with data.

Settings – risk the environment in which the data is shared risks unauthorised use or disclosure	
Risk	Risk of data breaches where the data storage, transmission and access is not secure. Once data leaves an organisation, control over what happens to that data is lost. The risks of loss of control increase where data is shared with third parties.
Mitigation	Data custodians can minimise unauthorised use, access or loss of data through implementing technical, organisational and procedural measures to ensure data is handled and managed in safe and secure environments. Data custodians must assess the technology-based controls for how data is stored, transferred and accessed, and ensure protections are proportionate to the risk profile of the data being used. For example, data users accessing detailed, de-identified unit-level data may need to undergo an authorisation process and appropriate training. In contrast, de-identified aggregate level data may be accessed more openly with less need for authorised user status.

Data – risk where protections are not applied to the treatments applied to the data	
Risk	Risk of disclosure, data breaches and harm to an individual or the community when data users do not apply enough controls to keep personal data safe, for example through treatment methods such as data minimisation, aggregation, or suppression. Risk of reducing the potential usefulness of data when data restrictions (control or treatment) are applied to a dataset.
Mitigation	Data custodians must balance the need to preserve and protect privacy while ensuring the treatment method does not reduce the utility of the shared data for the user. Information and instructions (including a data dictionary and metadata) from the data custodians and data stewards help data users to better understand the limitations and quality of the dataset before using it.

Output – risk where the data sharing output is not safeguarded before any further sharing or release	
Risk	Risk of results (such as in a publication, report, or a secondary dataset) leading to disclosure of personal information. Risk of further sharing, publishing or releasing the result for broader consumption, or to develop different output/s, than had initially been agreed. Risk of not identifying outputs up front where projects are exploratory or experimental. Risk of Freedom of Information requests leading to the project result being made public where not intended. Risk of invalid, unfavourable or undesired data insights, including being unpalatable to government.
Mitigation	Data custodians must ensure protections are applied to check and assess the output for any confidentiality, sensitivities, legal or privacy risks. The data custodian and data users must conduct a risk-based privacy impact assessment and/or an ethics review and clearance process where appropriate.

Ethics and data sharing

Data ethics focuses on how our data practice upholds ethical principles such as fairness, trust, responsibility, transparency and integrity. DAMA DMBOK defines data ethics as how we "procure, store, manage, use and dispose of data in ways that are aligned with ethical principles."[11] The Open Data Institute (ODI) defines data ethics as "a branch of ethics that evaluates data practices with the potential to adversely impact on people and society – in data collection, sharing and use."[12]

Sharing and reusing data has the potential to either benefit or harm our community, depending on the processes and safeguards we put in place, so it is important that we always consider the ethical implications of sharing data. Legislation and policy attempt to codify ethical principles of data governance and management practice, but the speed of technological advances mean that new and emerging data ethics issues are not always covered by existing law and policy.

Our data governance and management principles – in particular principles 3, 'we share and use data safely,' which requires us to ensure appropriate and ethical use of data in accordance with legislative and policy requirements – and the Five Safes data sharing principles can help to provide an ethics lens through which we can assess our data sharing. Additional points to consider include:

- use, sharing and re-use of data should benefit our community and particularly the individuals or cohort represented in the data;
- the methodology used to capture the data should be robust and ensure quality data; and
- if consent is required for data capture or use, consent should be explicit and informed.

Further detail on how we protect, and safeguard data is provided in the 'make data safe and secure' section of this Guide.

[11] DAMA (2017), p49

[12] ODI (2019), *Data Ethics Canvas*, available at: https://theodi.org/wp-content/uploads/2019/07/ODI-Data-Ethics-Canvas-2019-05.pdf

How do we improve data sharing?

The ACT Government is committed to safely sharing data in a way that manages risks to privacy and security. By acknowledging the complex policy and legislative environment around data sharing and learning from past efforts to breaking down barriers to data sharing, data custodians, data stewards and all directorate executives can create the enabling environment and practices needed to safely share data.

ACT Government data governance arrangements must consider the following five areas to enable and improve safe data sharing, including data containing personal information. Further detail is provided at Appendix III.

1. Data and information sharing legislation	Review, identify and understand existing privacy, secrecy and confidentiality provisions in legislative frameworks. Staff should understand the limits of what we can share under the relevant legislation, rather trying to establish what is and isn't permissible on a case by case basis. Data custodians establish clear and consistent advice on data sharing.
2. Develop strong governance, policies and guidelines	Establish directorate-level data sharing frameworks with supporting policies and strategies to operationalise them. Review and establish the right authorising environment to enable information and data sharing. Develop review and check points within directorates. Apply whole of government data governance and management principles and the Five Safes data sharing principles. Use **data sharing agreements.**
3. Establish a strong data culture	Establishing a strong data culture in directorates includes building staff data literacy, driving effective change management processes to break down cultural barriers and ensuring staff feel enabled and empowered to work with data in their roles.
4. Develop digital infrastructure that supports the safe sharing of data	Directorate information and technology staff and Executive Data Leads are responsible for enhancing and building technology that applies a 'data- and privacy-by-design' approach so that digital systems enable safe sharing based on permissions and in accordance with legislation, governance and policies. Directorate executives, with data custodians and data stewards, support capability development through training and work with internal and external partners to ensure systems are fit for purpose, accessible and enable safe data sharing by default.
5. Build strategic partnerships	Directorate executives, Executive Data Leads and all leaders including data custodians are responsible identifying and build strong strategic partnerships internally and externally to leverage the lessons, experiences, skills and knowledge of other organisations or jurisdictions and to solve complex policy or service delivery challenges.

Data sharing practice in the ACT is built on a strong foundation of privacy and security However, there is an opportunity to support directorates with unified approaches including processes, tools and technical systems. The information in the 'make data safe and secure' section of this Framework supports data custodians and directorate leaders to shape safe and secure ways to handle, use and share datasets they hold.

Open Data and Data Release

The ACT Government increasingly shares data by default across the spectrum from closed to open public release.

Open data is publicly available data that can be freely used, reused and redistributed by anyone without any restrictions. For data to be considered 'open', it must be easily accessible and published in an electronic, machine-readable format under a Creative Commons 4.0 International licence that permits anyone, anywhere to find, access, use, share and reuse the data for any purpose. All data has descriptive metadata associated with it.

The ACT Government released its *Open Data Policy* in 2016 with the goal to support economic growth and wellbeing of the community. Through this policy, the ACT Public Service is committed to making its data holdings open, unless there is a reason why it shouldn't be. In accordance with the policy, careful consideration is given to aspects of privacy and security and data is only publicly released after a rigorous assessment process to determine its suitability for publication.

The policy acknowledges that ACT Government Open Data is to be released *by default*, protected where required, and allowing users the right to share and remix data, unless there are strong reasons for not doing so. The ACT Government releases data including geospatial data by creativecommons.org/licenses (CC BY 4.0). Additionally, all attributions should be articulated as "Australian Capital Territory" as the legal entity. Attribution should not refer to Directorate or specific teams. This information including the data custodian accountable for the dataset can be placed within the metadata.

The ACT Open Data Portal (www.data.act.gov.au) hosts a wide range of datasets including administrative and service data (e.g. school enrolments), customer data (e.g. transport patronage) and location data (e.g. public art locations).

ACT Government datasets that are primarily geospatial in nature are hosted on the ACTMapi Open Geospatial Data Catalogue (http://www.actmapi.act.gov.au/). Data ranges from imagery and land information to education and sports facilities.

ACT Government open data is also discoverable on the Australian Government's open data catalogue at data.gov.au.

The following diagram outlines the benefits of making our data open to the public.

Figure 19 Benefits of open data for our community and for the ACT Government

Improving Open Data

Decisions about what data to publish are the responsibility of the data custodian, based on data availability and suitability for public release and community requests for specific data. Data that is released should be de-identified and aggregated to protect the privacy and security of our community. Further guidance on safe sharing an realise can be found in the Five Safes data sharing principles, discussed above.

Government data is shared and released in and via many different formats and mediums, but problems can arise when these are not conducive to efficient sharing. For example, data in PDFs is not considered open, unless it can be separately accessed in a useable and machine-readable format where it can be freely reused.

The ACT Government is continually sourcing, updating and publishing additional data for the community to use. Users can also suggest the datasets they would like to see on the portal. It is preferable that data is made open where possible and the public does not need to request permission to access data. Some data on the open data platform is provided directly from business systems or services, such as the NXTBus API and the Smart Parking API. The ACT Data Analytics Centre (ACTDAC) supports directorates to explore what data can be opened to the public.

Resources
to support work to improve data sharing

Steps to enablement	Improve Data Sharing
Objectives	• Safe and trusted data sharing and public release by default
Outcome	• Ensure authorised users access dataset (data sharing) • Improve accessibility, useability and transmission of data (data flow) • Build trust in government data use, reuse, sharing and release (social licence)
For Data Users	• Can access and work with required dataset to support decisions • Can establish the sharing arrangements with data custodians.
For Data Custodians and Data Stewards	• Can ensure authorised data users access datasets, for specified purpose • Can help ameliorate risks of data breaches.
Example activities:	• Build trust and confidence in Government's ability to use data appropriately and safely to meet community needs through meaningful and responsive engagement with empathy and demonstrate respect for the lived experiences and perspectives of people whose data we gather and use on their behalf. • Develop data privacy, ethics, and building trust approaches and methods • Establish data sharing arrangements, controls, and data release requirements including for some datasets conduct privacy impact assessment
Example resources and tools in congruent with DAMA DMBOK and Office of the National Data Commissioner Need to define who is responsible for 1) design the product 2) implement the product 3) maintain and improve the product	• **Data sharing principles** - Five Safes as risk framework • **Safe Data sharing and access** support including ACT Government data sharing arrangements and process eg data access pathways, data classifications, guidelines for data incident (breaches) of information security/confidentiality • OAIC Privacy risk and impact assessment • **Data Privacy considerations** to help share and use PII and sensitive data in a standardised and responsible way including privacy preserving and people centred data practice eg Data tags • **ONDC advice** https://www.datacommissioner.gov.au/data-sharing • Standardised Data Sharing Agreement with Data Sharing Principles eg https://www.datacommissioner.gov.au/resources/draft-data-sharing-agreement-template • Consent - ensure individuals' choice and control over how their data is used and take responsibility for ensuring the consent is informed. • Open Data Institute - Open Data Support • The ACT Open Data website enables the public to find and use for ACT Government data. • The ACT Government's Open Data Geospatial Catalogue also enables this for geospatial data on ACTmapi • The Australian Government's open data catalogue data.gov.au. • Open Data institute supports the building of an open, trustworthy data ecosystem, where people can make better decisions using data and manage any harmful impacts, including through training.

ENSURE QUALITY DATA

1	Adopt a data quality framework and standard.
2	Identify and document data quality issues.
3	Improve data quality and resolve issues.
4	Communicate quality issues and improvements.
5	Ensure staff have skills and capabilities to use data.

Data governance and management principles

We are community centred	**We are transparent and accountable**	We share and use data safely	We are skilled and capable
We make data discoverable	**We make data trusted and secure**	**We value data**	We make data open

Trust is integral to ensuring data quality, access and use. A lack of trust in the way data is collected, stored and shared can result in data being underutilised and reduce the potential to realise its benefits.

At a basic level, quality data means data is fit for its intended purpose and can be trusted for use in decision making. Data is considered high quality when it accurately and reliably represents real-world observations or constructs. Other characteristics of quality data include completeness, relevance and trustworthiness.

It is good practice for the ACT Government to use a range of data and information from various sources and in varying formats to make policy and practice decisions. It is important to ensure the data we use is relevant, appropriate, accurate, valid and reliable. The challenge is for data users and decision makers to ensure that the evidence used is robust, reliable and can be trusted.

There are two quality dimensions to consider: the data itself (are there any quality issues inherent in the data), and the methodological framework used (how was the data collected, produced and analysed). This section covers the former, and other sections in this document help us with the latter. It should aslo be acknowledged that poor quality data can be used by data users, if they are well-informed of the quality issues.

To support trusted use of data, we should:

- use a range of data and evidence rather than relying on a single dataset;
- be aware of quality variations within datasets;
- assess the quality of the methodological approach (was the data collection method rigorous, valid, reliable and objective; that is, are there inherent biases in the dataset); and
- when capturing data, ensure data collection method and systems meet requirements set out in data quality standards and frameworks.

To ensure quality data, it is also important to consider key data management functions and how these will be implemented. The introduction to data management functions on page 22, also known as the DAMA-DMBOK knowledge areas, provides further information.

Why ensure quality data?

The ease and extent to which data can be transformed and use to inform public services, policies and practice depends on its quality. With quality data (or ‘fit for purpose’ data), we can trust the information we use to deliver better outcomes through evidence-based decision-making, while poor quality data (inaccurate, incomplete or misleading data) risks inaccurate analysis or misinterpretation. Quality data enables us to improve the consistency and comparability of our datasets across government.

Quality data leads to quality outputs, including informed, data-driven decision-making that leads to better outcomes for our community. Poor quality data and outputs, including poorly informed decision-making, can harm the government’s reputation and risk eroding public trust.

In addition, legislative requirements in both privacy legislation and some portfolio-specific legislation require data custodians to ensure accuracy in personal information that is collected.

How do we ensure quality data?

Through first reducing the risk of poor quality data by applying data standards at the outset, making data quality issues known, fixing those issues and communicating data quality to data users we can:

- enable data users to use data with confidence and trust to inform decisions;
- reduce the risks of poor outcomes for our community, harm to the government’s reputation and erosion of community trust in government; and
- improve data analytics capability through more consistency and comparability across datasets.

However, identifying and improving data quality takes time and can be complex. Start with identifying data quality issues in the highest-value datasets then gradually remediate these issues. However, poor quality data should not be locked away until it can be fixed - often, data users can achieve high quality analytical outputs if we are simply *aware* of the quality issues in the dataset. We discover, recognise, and resolve quality issues when data is used, shared and reused.

There are five steps for data custodians and stewards to actively manage data quality:

1. Determine data quality standards and framework

First, directorate Data Custodians and Executive Data Leads should adopt a data quality framework or standard to inform and guide the directorate's data quality practice and management.

> Geoscience Australian defines data standards as "documented agreements on representation, format, definition, structuring, tagging, transmission, manipulation, use, and management of common data. The use of common terminology and common data element definitions enables the integration of databases, and promotes more efficient and effective use of data by users of commonly defined data from disparate sources."

Data Custodians and Data Stewards are accountable for ensuring datasets meet the quality standards (from collection through to use and reuse) and as such should measure, monitor and control dataset quality.

The data quality framework should be built around the data quality lifecycle that includes the stages: define; measure; analyse; improve; implement; and control.[13]

Some data quality standards will use different words for similar concepts. It is important that each directorate chooses a set of data quality standards, usually associated with the data quality framework the directorate has adopted, and that these are used consistently across the directorate. Data Custodians, Data Stewards and Executive Data Leads must also collaborate at a whole of Government level to determine standards and data quality that adequately enable data access, sharing and transfer. They must also inform data users of the quality standards applied to the dataset.

A data quality framework and adopted data standards will contribute to a data quality culture, where data quality is a key consideration from the outset of data capture and program design (ie. quality in, quality out). Data quality and requirements varies across the ACT Government, which can limit the extent to which data can be shared, linked and used. This is largely due to the broad focus in data collections including driven by national and international data standards such as MeTEOR through the Australian Institute of Health and Welfare or the GeoSciML and EarthResourceML as international data transfer standards for geological and mineral resources data. Several examples of data quality frameworks and standards are provided below under 'Resources'.

[13] See the New Zealand Ministry of Justice Data Quality Framework as an example https://static1.squarespace.com/static/5e21c300ec15d34ee6e45969/t/5e635de3b6faeb732cde6b11/1583570435364/New+Zealand+Ministry+of+Justice+Data+Quality+Framework+PDF (accessed 21 June 2020)

Data quality standards[14] might include the following example elements:

Accuracy	The data correctly represents 'real-life' entities. For example, it can be measured by comparison to a data source that has been verified as accurate.
Completeness	All data is present. For example, the dataset contains all the records expected and they are populated correctly.
Consistency	Data values are consistently represented within a dataset and between datasets, and consistently associated across datasets.
Integrity	The dataset is not corrupted and does not have missing or lost data.
Reasonability	The data pattern meets expectations based on what is known about the data. For example, based on a comparison with benchmark data.
Timeliness	Data is current and represents the most up-to-date version of the information.
Uniqueness	Entities are not duplicated within a dataset.
Validity	Data values are consistent with a defined domain of values, such as a reference table.

The Australian Bureau of Statistics (ABS) notes that quality is generally accepted as 'fitness for purpose', meaning an output should be assessed with reference to its intended objectives or aims. Quality is a multidimensional concept and the ABS proposes seven dimensions of quality: institutional environment; relevance; timeliness; accuracy; coherence; interpretability; and accessibility. According to the ABS "all seven dimensions should be included for the purpose of quality assessment and reporting. However, the seven dimensions are not necessarily equally weighted, as the importance of each dimension may vary depending on the data source and the context."[15]

When assessing the fitness of data, it is important to keep in mind where the data has come from and how and why it was collected. All directorate staff should proactively ensure that data is captured and managed using the chosen data quality standards. Data should be sourced from the most reliable source (public or private). Reference datasets, master datasets and metadata are essential to support establishing new datasets and to understand and assess the quality of existing datasets.

We need to also recognise that data does not need to be high quality before it can be used. In some cases, it is after data is used that we can identify whether it has quality issues and so plan to improve it. The data quality standard can help us to identify and recognise the quality of the dataset, and in turn shape its value.

2. Identify and document data quality issues

The second step is for data custodians and data stewards to identify and document data quality issues; starting with the most active and high-value datasets. They can assess the data quality against the chosen data quality standards (step 1) and use impact assessment and root cause analysis techniques. They should keep a data quality register to document whether the datasets conform to the chosen standards. The ABS recommends preparing a data quality statement when assessing the quality of data collections or product.[16]

Data custodians and stewards may develop a curated (enterprise) data model and map all the datasets to the data model. The curated data model should be simplified and easy to understand and enable users to build their own reports or queries.

[14] DAMA (2017), provides several examples of data quality standards, p455 – 459.
[15] ABS (2009) Data Quality Framework (cat.no. 1520.0)
https://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1520.0Main%20Features2May%202009?opendocument&tabname=Summary&prodno=1520.0&issue=May%202009&num=&view=

[16] https://www.abs.gov.au/websitedbs/d3310114.nsf/home/ABS+Data+Quality+Statement+checklist

3. Improve data quality and resolve issues

Third, managing the quality of our data is a continual process across the full data lifecycle, from capture to its potential destruction, and requires data custodians and stewards to have a proactive approach to monitoring and managing data quality. This a cyclical or ongoing process rather than a linear one, given that quality issues may only come to light as data is being analysed and used.

This begins with fostering a data culture where quality data is valued by data users, staff are trained and enabled to recognise and work with quality data, and data custodians and executives communicate openly and transparently about data quality. In a culture where data is valued, data quality issues are more likely to be noticed, acknowledged and addressed in a timely way.

Data custodians establish a data quality improvement plan to resolve identified issues, focusing on their most active and high value datasets. This plan will outline the agreed remediation actions and target dates, for example:

- *No Action*: data issues are small or not meaningful, and will not cause a problem.
- *Remediate during processing*: data issues should be remediated during data processing or transformation.
- *Remediate in source databases*: data issues should be remediated in the source database, for example by checking for invalid or unvalidated data entry processes or input into the software / database, and whether downstream users were notified of third-party changes.
- *Remediate in target application*: data issues should be remediated once the data has been loaded into the application.
- *Remediate in business process/rules*: data issues should be addressed at the point of capture or entry, checking for business rules being applied or changed.

Data custodians and stewards can employ other methods to improve data quality including: parsing and standardisation (validating and correcting data to the chosen standards, eg address validation); data enrichment (adding value through scoring and profiling); and data monitoring and providing feedback mechanisms for data users to inform data custodians of quality issues.

Data quality issues can often be best resolved at the point of capture. One important element is to ensure that whoever is collecting or providing the data, for example frontline staff capturing data directly or members of the community providing data through electronic means, understands the purpose of the data. This will help to ensure that data provided is relevant and complete.

Unresolved data quality issues for high value datasets will continue to be documented and made available for viewing by data requesters and data users.

4. Communicate issues and steps to improve data quality

Fourth, data custodians and data stewards are responsible for monitoring, reporting and communicating data quality issues to all stakeholders. This is an ongoing process – as issues are discovered and resolved, data custodians and data stewards must update the data issues register, monitor and report on the action plans, and communicate openly with data users (both past and present). Data quality issues and plans should also be communicated with the data governance and oversight body within the directorate, such as a data governance committee or the Executive Data Lead.

5. Ensure staff have skills and capabilities to use data

Finally, it is essential that staff have the skills to work with data. Even with quality data, we risk inaccurate analysis or misinterpretation if staff lack the appropriate skills for quality analytical work. Data custodians and data stewards are responsible for ensuring that data users have the appropriate skills and qualifications to use and analyse data.

Resources
to support work to ensure quality data

Steps to enablement	Make Data Quality Known
Objectives	• Improve quality of datasets • Build trust in Government data use • Improve consistent and comparability of datasets
Outcome	• Build trust in the ACTPS collection, storage, sharing, use and release of data and to support evidence-based decisions while striking a balance between compliance, productivity and safeguarding privacy. • Know where data fits in the data ecosystem (data architecture mgt) • Improve consistency and comparability of data (reference and master data) • Know the quality of the dataset (quality mgt) • Improve the quality and accuracy of the data and reporting (quality mgt)
For Data Users	• Can use data with confidence and knowledge about data quality. • Can understand data lineage and data relationships. • Can trust that new datasets will be established with quality at the outset.
For Data Custodians and Data Stewards	• Can identify data quality issues to data users • Can signal to Data Users that the dataset aligns with the data quality standards. • Can ensure authenticity, reproducibility and trust in datasets and understand the value of data as an asset.
Example activities:	• Identify data quality issues • Develop data profile • Establish Data Quality issues register • Develop data quality improvement plan using data quality standard • Establish enterprise Master data, Reference data, and Management. • Map dataset to the Enterprise Data Model and Master Dataset • Develop data operations manual • At the outset of new projects or initiatives or when reviewing and revising an existing one, apply design wheel with data dimensions

Example resources and tools in congruent with DAMA DMBOK and Office of the National Data Commissioner
Need to define who is responsible for
1) design the product
2) implement the product
3) maintain and improve the product
	• Examples of data quality standards and frameworks
	  ○ Australian Bureau of Statistics (2009) *Data Quality Framework* – includes seven dimensions of quality: institutional environment, relevance, timeliness, accuracy, coherence, interpretability and accessibility.
	  ○ The ABS Data Quality Management page helps identify and use the seven dimensions of the *ABS Data Quality Framework*:
	  ▪ define the quality of a data item or a collection of data items
	  ▪ assess the fitness for purpose of data in the context of a data need
	  ▪ identify data gaps and areas for future improvement.
	  ○ The Data Management Association (DAMA) Data Management Body of Knowledge (DAMA-DMBOK) – data quality dimensions
	  ○ ISO8000 is a global standard for data quality and enterprise master data.

	• Data architecture and data ecosystem
	• Master Data Management tools
	• Data provenance and lineage tools
	• Physical data model, common reference/master dataset model
	• Data, Digital and Design – combining data and digital with design thinking to create value
	  ○ Data lifecycle
	  ○ Data product development lifecycle
	  ○ ACT Government Design Wheel
	  ○ Design thinking, lean process and agile methods
	  ○ Change management and benefits realisation
	  ○ Digital, privacy and security by design

Other materials

- Chien, M (2020) *Getting Ahead of Data Quality with Gartner's Data Quality Operating Model*, Gartner Data and Analytics Summit, Gartner, p17.
- NSW Government data quality reporting tool that can be used to generate data quality statements in various document formats.
- https://www.dataqualitypro.com/ is free to join and provides a suite of resources for data quality practitioners
  - How to create Data Quality Frameworks, Policies or Methodologies https://www.dataqualitypro.com/blog/how-to-create-a-data-quality-framework
  - Data Quality Rules: The Definitive Guide to Getting Started https://www.dataqualitypro.com/blog/data-quality-rules-guide?ss_source=sscampaigns&ss_campaign_id=5e7df398af20545fc9f142d3&ss_email_id=5eef32f44f2328627591d0af&ss_campaign_name=Data+Quality+Rules&ss_campaign_sent_date=2020-06-24T10%3A14%3A06Z
- Data Ecosystem includes the Consumer Data Right (CDR) being established by the Australian Competition and Consumer Commission (ACCC) as lead regulator of the CDR, supported by the Office of the Australian Information Commissioner (OAIC).
  - The CDR is intended to be applied sector by sector across the whole economy, beginning in the banking, energy and telecommunications sectors.
  - The consumer data standards have been developed to facilitate the CDR by acting as a specific baseline for implementation. https://consumerdatastandards.gov.au/
  - Further information on the CDR is available on the CDR website, the ACCC website, and in the Explanatory Memorandum to the CDR Bill.

MAKE DATA SAFE AND SECURE

1	Establish safe data practices, technology and controls.
2	Build trust in government through safe data use.
3	Support staff to know their responsibilities to implement records, privacy and security by design.
4	Establishing directorate-level data protection, including data breach response plans.

Data governance and management principles

We are community centred	**We are transparent and accountable**	**We share and use data safely**	**We are skilled and capable**
We make data discoverable	**We make data trusted and secure**	**We value data**	**We make data open**

The ACT Government is committed to ensuring the data and information that we hold on behalf of the community is managed and governed in a way that keeps it safe, secure and reliable throughout its lifecycle. This section of the Framework provides a guide to data protection measures relating to the data itself, the systems we hold it in, the technology we use it with and the people who use it.

This Guide specifically identifies the preservation of privacy and the security of personal and sensitive data as a core principle. Whether we are collecting data to provide Canberrans with the services they need every day, working with data to inform policy planning, releasing data on open data or building secure information and data sharing capabilities, ACT Government directorates are obligated to maintain the safety, security and privacy of data in our activities.

SAFE	Making data safe means protecting the privacy and safety of the people the data is about. It is about removing data that is sensitive or that could identify individuals.
SECURE	Making data secure means ensuring data is protected from unauthorised access, harm (corruption) or loss (deletion) while remaining accessible to authorised users. It is about the controls we put in place around the systems in which the data is kept.

Why make data safe and secure?

As community expects more accessible, responsive and personalised services from government, the ACT Government is improving and increasing its use of new and emerging data and digital technologies. With greater data use come risks to safety and security, and the need to build and maintain public trust in our ability to manage data while protecting personal information and safeguarding privacy. This includes protecting the data infrastructure we rely on.

Better outcomes for our community

We use data to deliver better outcomes for our community, through understanding community needs and what can help to address those needs. We ensure data is safe and secure so that we can trust it to use in decision-making, leading to better policies, programs and services for the community.

Sharing data is another way we deliver better outcomes for our community, so it essential that we also have systems and processes in place to ensure data is safe and secure when it is shared.

Protecting our community's privacy and personal information

Some of the data we use to understand community needs may include personal or sensitive information, such as observations about an individual's lived experience, their personal characteristics or circumstances. By making data safe and secure we are protecting the privacy and security of our community and helping to ensure that decisions and actions we take based on that data are transparent and accountable.

Building trust in government

One of the outcomes from our data vision, purpose, and principles is to keep **the community's needs front of mind and earn their trust when using and protecting their data and information**. This means that the community trusts that we use data responsibly, ethically, and in the public interest, and that the choices we make about what data we collect, how we manage and use it, are just, open, and honest.

We earn and maintain this trust by acting fairly and responsibly, and by demonstrating that we are competent and have proactive security processes in place to protect their personal information. We use data ethically and are transparent about what we do with data. We communicate, engage and build good relationships with stakeholders, listen to community views including people who are impacted by our decisions. We respond quickly when things go wrong, are honest about mistakes and learn from them.

These practices are outlined in the four Trust Principles developed by the Australian Data and Digital Council: Respect, Security, Accountability and Transparency.[17] The ACT Government, like all jurisdictions, is applying these principles to guide our actions as we design and deliver using data and digital technologies.

Respect	Security	Accountability	Transparency
• Act fairly and ethically • Make engaging with us easy and listen to your views	• Protect your privacy • Implement strong security systems	• Be honest about mistakes and learn from them • Respond quickly when things go wrong	• Proactively communicate with you • Where safe to do so, provide data openly to the public

Trust in Government Data Use – Toolkit
(Department of Prime Minister and Cabinet, 2019)

- *Government data capture, use and protection practices are largely opaque to the public.*
- *Security concerns and trust in government's ability to safeguard data holdings is a key concern for the public.*
- *Government is not perceived as being particularly competent when it comes to protecting members of the public's data.*
- *There is a pressing need to raise public awareness of how data is being safeguarded.*

Who is responsible for making data safe and secure?

The 'identify data roles and responsibilities' section of this Guide helps us to identify the staff responsible for ensuring data protections are in place, including in the event of a data breach.

Depending on the directorate's structures and functions, there may be different requirements for different areas. For example:

- the Executive Data Lead, senior executives, and senior managers might be responsible for building a 'privacy aware' culture and establishing policies and procedures with data protection in mind;
- the Chief Information Officer, business owner, directorate embedded ICT teams and SSICT who develop, design, select and use applications, business systems and system architectures that process personal data must consider data protection requirements; and
- corporate, policy and program staff, including those with specific data functions and roles (such as data custodians and records officers), should embed data protection by design in all business operations, processes and procedures.

Directorates are responsible for improving privacy, security, records and risk management capabilities. As such, all executives and the Executive Data Lead are responsible for establishing learning and development opportunities for directorate staff, which might include: being privacy-aware and identifying risks to data integrity and individual privacy; understanding the Territory Privacy Principles; embedding privacy and recordkeeping protections in data practice, infrastructure and systems; and knowing what to do in the event of a data breach or security risk. Staff should also be supported to know when to seek technical advice.

[17] https://www.pmc.gov.au/sites/default/files/publications/addc-trust-principles.pdf

How do we make data safe and secure?

Making data safe and secure, should be a feature in everything we do. All directorates must establish appropriate technical and non-technical measures to implement an organisation-wide approach to safeguarding individual privacy. We must also clearly understand the role our data plays in supporting and documenting our actions and decisions, so that we can ensure its integrity and be accountable to our community.

Data and records privacy and security *by design*

We use a 'records, privacy and security by design' approach when dealing with data across the entire lifecycle, from the initial design stage through to developing and delivering any system, policy, program or service. We start by considering the intended purpose, scope, context and nature of the data activity, its relationships with other business processes, and any potential risks this may pose to the privacy and safety of individuals. From a technical point of view, the *Shared Services Information Security Assessment tool* can help frame this thinking.

We can protect data by ensuring that we:

- understand and embed the Territory Privacy Principles (TPPs).
- establish privacy protections throughout the data lifecycle, for example by:
    - specifying privacy requirements for data and digital systems and applications (eg default settings);
    - creating and enhancing data security features in applications and systems architecture;
    - ensuring and testing that adequate security features are in place in systems that are not under direct control (e.g. cloud systems managed by external vendors);
    - ensuring data is captured and stored in a system that is appropriately protected against attack;
    - ensuring data is only accessible to those who need to use it; and
    - ensuring that data (including open data) can only be changed through authorised processes.
- build privacy and security assessments into the whole data lifecycle. Threats will change and evolve over time, and controls must be checked, tested and adapted to remain useful. Security and privacy should not be 'set and forget'.
- Undertake recordkeeping analyses to:
    - understand when data is used as part of the Directorate's business transactions and may form a record of those actions.
    - ascertain the significance of those data assets to the business and the community.
    - ensure that relevant systems and processes are built to protect the integrity and document the ongoing management of records in accordance with their significance and other requirements.
- support staff to know their responsibilities and obligations when working with data;
- include data-safe practices in directorate data governance and management implementation strategies, for example:
    - conduct regular threat risk assessments and system security accreditation processes;
    - conduct privacy impact assessments to identify and reduce risks and improve processes for handling personal data, including whenever there is a new or changed process or system;
    - conduct recordkeeping appraisals and assessments as part of all systems design or procurement processes to ensure that recordkeeping needs and expectations can be met;
    - minimise the use and processing of personal data and -identify personal data as soon as possible; and

    - implement privacy-enhancing or privacy-preserving technologies that minimise personal data use and maximise data security.
- establish a directorate-level, and if required a project-level, data breach response plan; and
- communicate and engage with the community on data use including the use of personal data.

Territory Privacy Principles

Data use in the ACT Government is governed by a range of legislation including the *Information Privacy Act 2014* (ACT), which contains 13 Territory Privacy Principles (TPPs) that set out our obligations for managing personal information. The TPPs are:

- TPP 1—open and transparent management of personal information
- TPP 2—anonymity and pseudonymity
- TPP 3—collection of solicited personal information
- TPP 4—dealing with unsolicited personal information
- TPP 5—notification of the collection of personal information
- TPP 6—use or disclosure of personal information
- TPP 8—cross-border disclosure of personal information
- TPP 10—quality of personal information
- TPP 11—security of personal information
- TPP 12—access to personal information
- TPP 13—correction of personal information

The TPPs are based on the Commonwealth Australian Privacy Principles (APPs) with slight differences. The ACT does not have TPP 7 and TPP 9, although in some exceptional cases APPs 7 and 9 may apply in the ACT. The ACT Government is not currently an APP Entity under the *Privacy Act 1988* (Cth) for the purposes of the APPs. At times, however, certain personal information held by our contractors and ACTPS staff personal information held by HR areas may be governed by the *Privacy Act 1988* (Cth).

Document, Record and Content Management

These are activities that help us to better manage, store, protect, and access data found within electronic files and physical records (including text, graphics, images, audio and video).

The strategic direction of **Records Management** as an essential whole of Government function is set and supported by the Territory Records Office under the *Territory Records Act 2002*. Records management policy and governance are defined, with Directorate records officers and staff responsible for records management.

Document Management involves the classification of documents as records, with unclassified documents (or working document) generally unmanaged. Staff and teams are responsible for establishing consistent naming conventions, folder structures on shared network drives or SharePoint for managing, archiving, deleting, and sharing documents that are relevant to the business functions. Teams are accountable for improving their document management practices and to minimise document duplication in terms of storage and sharing (eg via emails).

Directorates maintain a broad and varied set of internet and intranet sites, pages and documents that require **Content Management**. This includes ensuring good governance around web content publishing and maintenance, as well as addressing Government policy.

Data is safe

One of the ways of we make data safe is through removing, where possible, all sensitive and personal information before the data is accessed, shared, used or published. However, in practice, there are often

legitimate reasons for datasets to retain personal and sensitive information while being accessed. In such cases, we apply controls to make the data as safe as possible while still maximising its utility and value. The Five Safes data sharing principles can help mitigate potential data sharing risks.

Examples of controls to keep data safe while it is accessed and used	
De-identification	Remove personally identifying details such as a person's name or date of birth, or any unique characteristics that may make them identifiable.
Aggregation	Group or summarise the data, for example by 10-year age groups or by suburb.
Masking	Replace some or all characters within a field with another character. For example "#### #### #### 2356" for a credit card number.
Perturbation	Use statistical methods to add deliberate errors (noise) to a data set so that overall the data retains its characteristics but at an individual record level the data is no longer accurate.

We take a risk management approach to applying controls. This means we identify the risks, their likelihood and their consequences and then choose the most effective treatments for the dataset given the context. A treatment may be made up of one or more controls that, when applied, reduce the likelihood or consequence of the risk. Further information about risk management approaches can be found in the *ACT Government Risk Management Policy 2019*.

We can apply different controls for different uses of the same dataset. For example, we might de-identify data before it is used for analysis and reporting, but we might retain people's names and addresses and remove their clinical information for a bulk mail out to health service recipients. This helps to ensure that only data elements and records that are required are accessed and used, while removing those that are not required. All staff should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming re-identifiable or 'reasonably identifiable'.

When data is shared or released through open data, we apply more stringent controls, which are incorporated into the broader governance approach to sharing and release. We support effective risk management through ensuring that any data that includes sensitive or personal information is tagged (classified) appropriately. Classifying data according to what it includes and its purpose can help us to identify the level of protection required for the data and the systems or devices on which it is stored, in order to protect it from unauthorised use or accidental modification, loss or release.

Further information about how we classify information to determine the correct level of risk can be found in the *ACT Government Protective Security Policy Framework: Information Security Guidelines*.

Re-dentification through contextual features

All data has context; for example, when an event occurred (e.g. day or hour), or where it occurred (e.g. street, suburb). Individuals can be connected to other people, objects or the broader population through their relationships (such as family or cultural group, partnership).

Despite every effort to protect personal information in a dataset, such as through de-identification, there remains a risk of re-identification if a data user can link or combine enough contextual features to make inferences about the person. That is, a person may be identified based on combining a minimum set of identifiable features (e.g. eye colour, gender, age, address). When enabling data access, data custodians should always consider the privacy protection approaches to be necessary to mitigate the risk of re-identification.

Data is secure

Data security is about ensuring data is available to authorised users and is kept safe from harm (corruption) and loss (deletion) while remaining accessible to users. Data security often involves technical assessment and expertise to understand the best controls to be applied given the specific risk/threat environment.

The *ACT Government Protective Security Policy Framework: Information Security Guidelines* sets out how to implement data security within the ACT Government risk management context. It is derived from strong federal and international standards (Australian Signals Directorate's Information Security Manual[18] and ISO27001[19]) that assist in choosing the best combination of controls to reduce specific risks. To understand the best combination of controls to ensure data security, we consider the *ACT Government Protective Security Policy Framework* and work together with relevant technical experts to understand the technical risk and controls in terms of the business context.

The Territory Records Office *Standard on Records, Information and Data* and its supporting guidelines also provide a framework in which to make decisions about the management of data, in the form of records, that provides evidence of government activities. Records are vital to protect the rights and entitlements of government, the community and stakeholders, to support business continuity, to contribute to the community's trust in government by supporting audit and other accountability measures, and to document the history of the ACT and the impact of government activities on individuals, groups and the environment.

It is particularly important to ensure that data systems and processes that create or manage records can protect them from alteration, corruption and unauthorised disposal. The design of protections should be commensurate with the significance of the records being protected and the risks to government or the community of not being able to access or rely on those records when needed. Current privacy and security considerations are obvious risks to be managed. Other important considerations are the length of time records need to be retained and the context in which they may need to be made publicly available.

Examples of good practices that facilitate data security include:

- establishing controls or treatments, such as:
    - backups
    - encryption over wire (transit)
    - encryption at rest (storage)
    - role-based accessed controls for creation, reading, updating and deleting of data.
- maintaining records and providing information to potential data users on the purpose of the data and the privacy, security and legal basis of the data holding;
- establishing an audit log retention and management approach to monitor access and demonstrate the integrity of data;
- applying and documenting records and data retention schedules to ensure that data is retained for as long as needed, but no longer;
- establishing robust controls over authorisations and processes for data deletion that support transparency and accountability;
- considering how data will be kept secure both in transit and where it will be stored when it is extracted (copied) from its original source;
- identifying and enabling freely given, specific, informed and unambiguous consent from data providers;
- Using the Five Safes framework to guide data sharing and release activities.

[18]Australian Government Information Security Manual <https://www.cyber.gov.au/ism>
[19] ISO27001 Information Technology - Security techniques — Information security management systems — Requirements < https://www.iso.org/standard/54534.html>

Proactive and responsive data breach practice

A **Data Breach** occurs when personal information or protected information held by the ACT Government is subject to unauthorised access or disclosure or is inappropriately lost or accessed. Section 12 of the *Information Privacy Act 2014* defines a privacy breach as 'an act or practice that breaches a Territory Privacy Principle (TPP)'. A data breach can also be known as a 'data security incident' or 'privacy breach'. Data breaches require additional management and response on top of what would take place following a data security incident. Data breaches can occur even when staff are vigilant and proactive. A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

When a breach of personal information occurs, as set out in the TPPs, it may be a notifiable breach if it contains TFNs or in some cases where personal health information is present (as defined by the *Health Records (Privacy and Access) Act 1997*, meaning it falls under mandatory reporting requirements specified by the Office of the Australian Information Commissioner. Although the ACT does not have mandatory reporting requirements to the same extent as the Commonwealth[20], we must still act decisively and respond quickly to minimise potential harm, manage further risks, and openly and proactively communicate with the public.

Directorates must prepare data breach response plans to enable quick and transparent responses to a data breach, mitigate the impact on individuals, reduce the cost of dealing with a breach, ensure that the directorate can learn and improve, and continue to preserve and build public trust in its operations.

Data breach examples

Data breaches can range in size from an incident that impacts just one or a few individuals, such as losing a page of names and phone numbers, to incidents that impact large groups, such as unauthorised access to data system containing multiple datasets from across government. Examples of data breaches include:

- loss or theft of physical devices (e.g. laptops) or paper records containing personal information;
- unauthorised access to personal information by an employee;
- disclosure of personal information due to 'human error' (e.g. an email sent to the wrong person) or as a result of inadequate identity verification procedures (e.g. to a scammer);
- incorrect configuration of access controls, meaning data is exposed to unauthorised users; and
- download of personal information from data storage to insecure mediums such as shared drives.

Information on cyber security incidents are defined in the *ACT Government ICT Security Incident Response Plan 1.4*. If any of the following occur, the potential for a data breach should be immediately investigated through enacting the data breach response plan:

- a user is tricked into entering their credentials into a page that mimics a legitimate site;
- a brute-force (automated trial-and-error) attack on username and password combinations is performed against a service;
- a service is compromised, and credentials are stolen and used to access the system or tested against other sites such as social media and email;
- a user's system is compromised by malware designed to steal credentials; or
- a staff member suspects that there is an active cyber intrusion into ACT Government systems.

[20] Because the ACT Government is not an Australian Privacy Principles Entity under the *Privacy Act (Cth) 1988*, ACT public sector agencies are not required to report to the Office of the Australian Information Commissioner (OAIC) under commonwealth's the Notifiable Data Breach scheme (NDB).

Directorate Data Breach Response Plans

Directorate Executive Data Leads are responsible for proactively preparing directorate-level data breach response plans before any incident occurs. Given the broad range of possible data breach incidents, there no one-size-fits plan for dealing with a potential data breach. To ensure the data breach response plans are suitable to the directorate's context, Executive Data Leads will design the plans with data custodians, data stewards, other directorate executives, directorate privacy officer, the chief information officer, SSICT Security team and the whole of government Chief Digital Officer. The Chief Digital Officer is also responsible for communicating data breach incidents to the community on behalf of the ACT Government.

Data breach response plans need to be widely shared and communicated with all staff to ensure broad understanding and support. Directorate data breach response plans set out how the directorate will respond in the event of a data breach. They should address questions such as (but not limited to):

- **Who** is responsible for dealing with the data breach and who needs to have input?
  Clearly set out the responsibilities of staff in specific roles including:
  - Who in the directorate needs to be informed about the data breach?
  - What is the responsibility of a data custodian or a data steward in in the event of a data breach?
  - If the data breach is likely to impact other directorates or external parties (for example, an external data custodian), how will the directorate engage with them?
- **How** will we work together to determine what needs to be done to minimise harm and respond to this specific context?
- **Why** should certain actions be taken?
- **What** needs to be done to respond from a legal standpoint and from a principles-based data governance standpoint?
- **What** lessons do we need to learn and apply from this breach?
- **When** do actions need to be taken ensure the effectiveness of the *what?*

The ACT Government applies the OAIC's data breach preparation and response advice which includes the following steps.

Data breach	Staff, contractors or external party alert directorate to suspected or actual breach.
Staff member or contractor	Immediately notify line manager, executive and data custodian about the breach. Record time and date of the breach, type of information involved and context, cause and extent of the breach.
Executive	Determine whether a breach has or may have occurred. Determine if the data breach and its potential impact requires escalation to the data breach response team, notify Executive Data Lead and privacy officer.
Data breach response team	Directorate privacy officer establishes data breach response team, including data custodian and steward, Shared Services ICT Security and Executive Data Lead. 1. Contain the breach 2. Assess the risk for individuals and take steps to remediate risk of harm 3. Consider who must be notified 4. Review incident and take action to prevent future breaches.
Executive Data Lead	Evaluate how the data breach occurred and the success of the response to help improve future data handling and data breach management in the directorate and across ACT Government.

Engage with the community

We are committed to proactively engaging with the Canberra community to understand the public benefits of data use, actively respond to privacy concerns, and be open and transparent about how we use data and how we are protecting personal information.

Directorates are encouraged to:[21]

- be clear about how information being captured is used and protected under existing legislation;
- provide easier ways to for people to manage their personal information and give or remove permissions;
- seek consent to capture the data (depending on the purpose or the target group);
- ask permission to reuse or share personal information where there is no existing authorising legislation to help people to make an informed choice to consent the use of their personal information;
- provide alternative options for people who choose not to have their personal information reused;
- be open and transparent about data we use for research, policy and analytics purposes and how that data is protected and secured, particularly for new data analytics projects; and
- collaborate with people in the community to understand and keep in touch with the range and strength of attitudes to privacy and data sharing, to help make the best-balanced choices around how data is used.

[21] ACT Digital Strategy, available at <https://www.cmtedd.act.gov.au/digital-strategy/data>

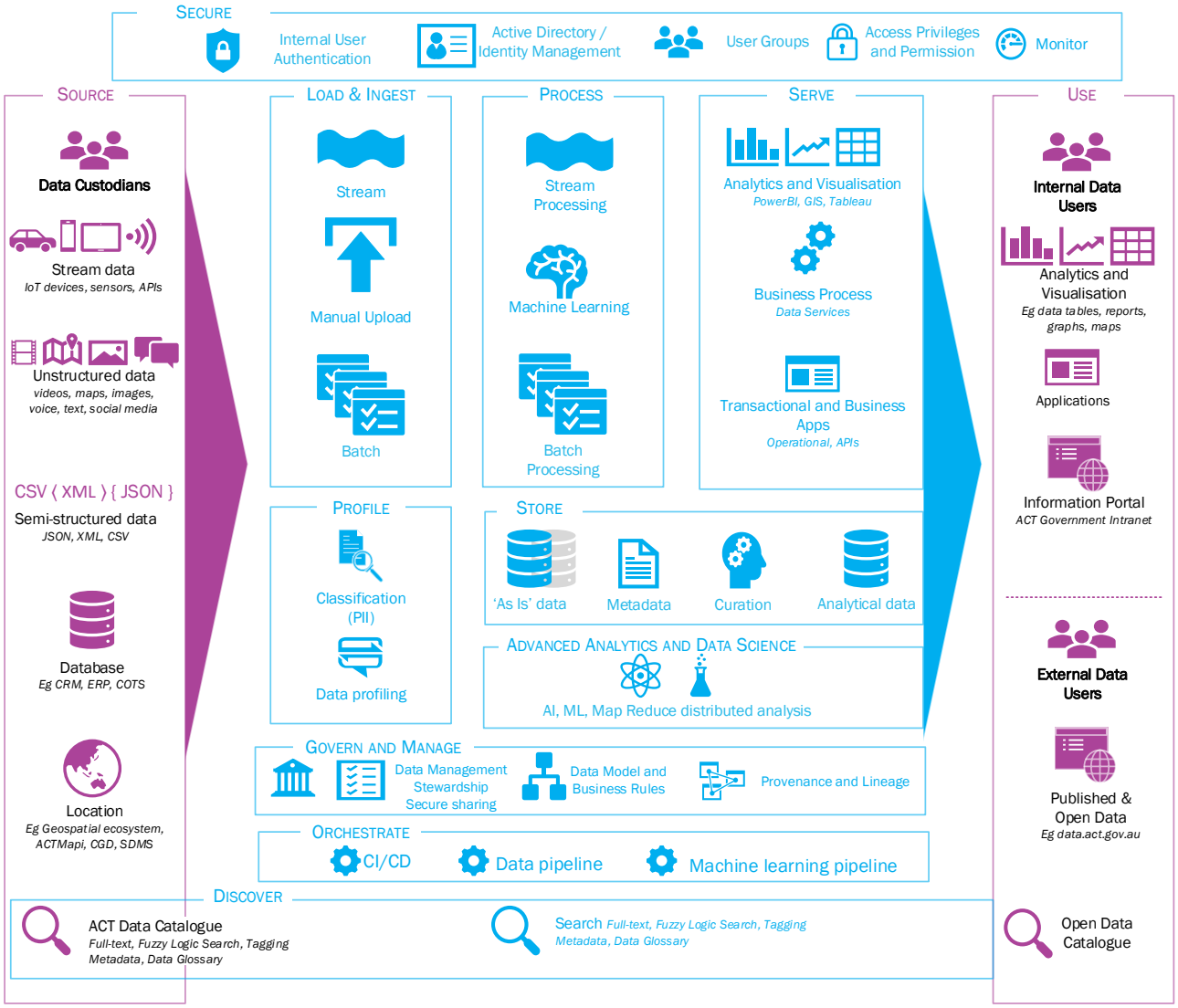
Data architecture, warehouse and business intelligence

Data architecture refers to the models, policies, rules or standards that govern which data is collected, how it is stored, arranged and used in a database system and/or in a directorate. It is an important part of the data management framework.

In a typical data architecture, transactional data moves from data providers, data producers and data custodians and operational and other source systems to a central facility such as a data lake and a data warehouse where data can be integrated. It further moves through data mart or storage for delivery into the analytics layer to be consumed by data users in the form of reporting or analytics. Metadata, master and reference data, data quality, data governance, data security and data privacy all play a critical role across the entire flow of data along the architecture layers.

Data architects work with data management roles to help design and optimise data architecture across all layers.

Figure 20 Generic Data Architecture



Resources
to support work to make data safe and secure

Steps to enablement	Make Data Safe and Secure
Objectives	• Build trust in Government data use • Protect the safety, privacy and confidentiality of individuals and businesses
Outcome	• Build trust in the ACTPS collection, storage, sharing, use and release of data and to support evidence-based decisions while striking a balance between compliance, productivity and safeguarding privacy.
For Data Users	• Can safely and securely access, receive and use data.
For Data Custodians and Data Stewards	• Can ensure safe and secure sharing of data with data users • Can help ameliorate risks of data breaches.
Example activities:	• Embed a security, privacy and safety by design practice and requirements such as access and security controls when collecting data, storing data, using data, sharing data and releasing data. • Work closely with agency and SSICT security experts • Identify provenance for high-value datasets • Embed data security controls and procedures around classification, access and publishing • Manage database operations including cloud • Manage data as a record: document, content, records and information management
Example resources and tools in congruent with DAMA DMBOK and Office of the National Data Commissioner Need to define who is responsible for 1) design the product 2) implement the product 3) maintain and improve the product	The following resources support work to make data safe and secure: • **Document, Record and content Management –** activities to manage, store, protect, and access data found within electronic files and physical records (including text, graphics, images, audio and video). • ACT Government Risk Management Policy 2019 • ACT Government ICT Security Policy • ACT Government Protective Security Framework • ACT Government Information Security Assessment • The Territory Records Office assists Territory agencies to meet their Records Management requirements as set out in the *Territory Records Act 2002*. • The Office of the Australian Information Commissioner data breach preparation and response resources can be used to support each directorate's data breach plan • Seven 'foundational principles' of Privacy by Design are provided at Appendix IV. • Make data safe to share and use through de-identification, privacy preserving methods and tools, data linkage and data integration approaches, Accredited data authorities, data ethics supports eg canvas and Data ethics resources • More information on the concepts of data integration and the separation principle can be found on the ABS, National Statistical Service and Department of Social Services websites

Resources from the ACT Territory Records Office include standards and guidelines for records, information and data.

Additional resources at can be found in the following guide from the Australian Government *Trust in Government Data Use Toolkit*.[22] It is important that data users check for the most up to data versions of resources, however this list provides a good starting point to seek further information about keeping data safe and secure.

Data Collection	Data Storage	Data Use	Data Sharing	Data Release
• Department of Finance – Commonwealth Risk Management Policy • OAIC – Privacy Act guidance • Australian Code for the Responsible Conduct of Research • NAA – Information Management Standard	• ASD – Australian Government Information Security Manual • OAIC guide to securing personal information • DTA – Secure Cloud Strategy • NAA – Disposing of Information	• ABS – Confidentiality series • High level principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes • National statement on Ethical Conduct in Human Research • OAIC Guidelines on Data Matching in Australian Government Administration • Guidelines section 95A of the Privacy Act 1988 (Cth) – Health Research	• ONDC – Sharing Data Safely • OAIC – De-identification and the privacy act • Data61 – a framework for de-identification	• OAIC Freedom of Information guidance • Open public sector information • NAA Archives Act guidance

[22] Commonwealth of Australia, Department of the Prime Minister and Cabinet (2019), *Trust in Government Data Use –Guide and Toolkit.*

Part III – A MODEL TO MEASURE DATA MATURITY

MEASURE DATA GOVERNANCE AND MANAGEMENT CAPABILITIES

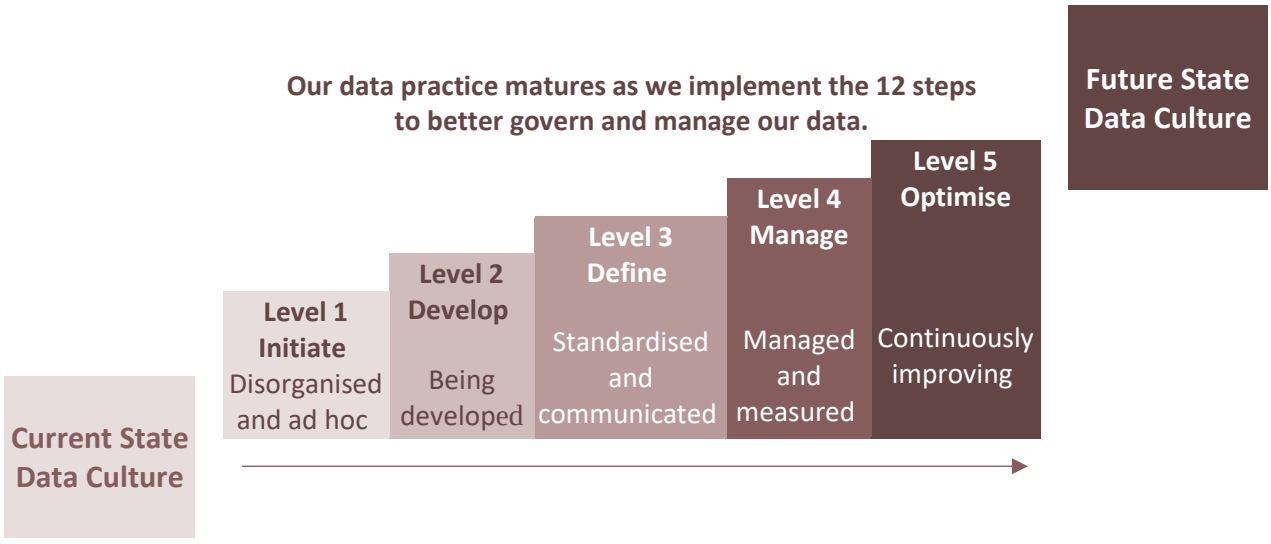
Directorates have already begun a step change towards a data-driven ACT Public Service. This has included making decisions about the future of work and leading digital transformations of legacy operations. We are working to reduce manual and paper-based processes, using tools such as customer relationship management platforms to deliver client-centred services, and sharing data within and across directorates for joined-up policies and services. These types of activities are building our *fitness* for a data- and digitally-led organisation, and helping us to change the status quo in: what we do, how we work and what we value.

We are committed to using data to drive forward policy advice and service reform, improve service delivery and know our impact. Data is a now a fundamental tool that digital technology has greatly enhanced. We accept that if we do not grasp it, we run the risk of becoming less efficient and effective.

So, as we progressively implement the framework's 12 steps to improve data governance and management, we will move closer to a collective culture where we can safely acquire, use, share and release data within and between directorates, particularly where sensitive information is involved. This Framework and guide will help us to ensure directorates retain full control over how our data assets are used and by whom.

Our data governance and management implementation strategies and associated roadmaps will help identify the case for change, the current state of our data efforts and improvement journeys. They will help our organisations get into shape – to be fit for a new way of working within a data culture. However, to achieve this level of transformation is more than being about a journey towards a destination. We must accept that the change we are working towards requires our ongoing and enduring effort, to continue to increase our levels of discomfort, and to shake our legacy foundations. We also accept that we need to maintain the change as we build our maturity and gain mastery in data practice.

For example, in some directorates, datasets currently exist in file structures and systems, with low visibility and sharing. Overtime, we will begin to transition from a current state of ad hoc and inconsistent management to a mature state where data is consistently governed, discoverable, understood, shared, high quality, and safe and secure. The following five levels can be used to assess our data governance and management maturity: Initiate; Develop; Define; Manage; and Optimise.



Appendix II provides the detailed measurement model to be applied at the outset of identifying the current state and future desired state of data culture and practice.

Measuring our data governance and management maturity

By using a levels-based maturity model, directorates and ACT Government can identify the maturity at commencement of our data journey, and to enable us to focus on key strategies and steps to improvements and rewards-based effort to accomplish desired activities, engage staff and executives, and communicate status.

Directorates are encouraged to define their current state and progress each year against the steps for better data governance and management. For a sample directorate, this might look like:

	2020	2021	2022
Establish Directorate Data Vision and Purpose	2	4	5
Know the ACT Policy, Legislation and Risk Context	2	3	4
Know the ACT Data Principles	2	4	5
Establish Directorate Data Governance	2	4	5
Identify Data Roles and Responsibilities	2	4	5
Establish A Culture That Values Data as an Asset	1	2	3
Make Data Discoverable	2	3	5
Make Data Understood	2	3	4
Improve Data Sharing	3	3	4
Ensure Quality Data	2	3	4
Make Data Safe and Secure	2	3	4

This could then be plotted on a graphic such as the sample graphic below, showing measurement of progress and change in directorate data maturity over time.

Data governance and management maturity measurement model

	Level 1 Initiate	Level 2 Develop	Level 3 Define	Level 4 Manage	Level 5 Optimise
	Disorganised and ad hoc	Being developed	Standardised and communicated	Managed and measured	Continuously improving
PART I – A DATA-DRIVEN CULTURE					
Establish Directorate Data Vision and Purpose	Undeveloped and not shared across Directorate	Directorate data vision is established	Directorate data vision is shared and embedded in strategies and plans.	Directorate data vision is seen in behaviours and executives review progress.	Unified Directorate data vision and data assets are continually enhanced.
Know the ACT Policy, Legislation and Risk Context	Poor or inconsistent awareness and understanding of data experiences, risks and barriers.	Establishing context for data practice, privacy and security including barriers to achieving the data vision.	Clarity of data risks and data practice including data and information sharing.	Executive actively manage data risks.	Unified understanding and application of data practice to manage and mitigate risks.
Know the ACT Data Principles	Inconsistent models in handling and using data.	ACT Data Principles acknowledged.	ACT Data Principles defined for day to day practice.	ACT Data Principles are present in day to day behaviours.	Unified set data principles across all data assets and practice.
Establish Directorate Data Governance	Undeveloped, and/or inconsistent data governance in directorate structures.	Directorate data governance structures established.	Directorate data governance bodies oversee data policy and practice.	Data Governance is embedded in Directorate structures and processes.	Ongoing feedback loops to enhance Directorate data governance arrangements.
Identify Data Roles and Responsibilities	Ad hoc and unsupported data capabilities and literacy.	Data capabilities defined and supported; executive data lead appointed.	Data roles assigned to every dataset and active data capabilities program	Staff routinely build data capabilities and positions describe data specific roles.	Ongoing feedback loops to enhance data capabilities, roles and responsibilities.
Establish A Culture That Values Data as an Asset	Undeveloped, not shared, and/or inconsistent data culture.	Desired data culture is being identified and existing barriers to data culture identified.	Data culture is defined in directorate strategy and leaders commit to change journeys.	Data culture is embedded in day to day behaviours.	Unified data culture. Subject to review & improvement.
PART II – A MANAGED AND MATURE DATA PRACTICE					
Make Data Discoverable	Data is in silos, disorganised & poor visibility.	Datasets are being identified and registered.	High value datasets are findable and accessible.	Management actively engaged in data discoverability.	Datasets maintained, updated and publicised.
Make Data Understood	Ad hoc and unsupported data documentation.	Dataset documentation processes being established.	High value datasets described, and new datasets are defined at capture.	Dataset described in machine-readable format and data is modelled against an enterprise data model.	Continual improvement of data definition processes & capabilities.
Improve Data Sharing	Data is accessible only to a small group or locked down.	Data sharing (Five Safes principles) arrangements being developed.	Well defined data sharing arrangements and facilities.	Data routinely shared using five safes data sharing principles and agreements.	Continual improvement and communication of data sharing infrastructure.
Ensure Quality Data	Data quality is ad-hoc. and the potential for reusability is limited.	Data quality framework and standards are established / adopted.	Data quality issues defined.	Data quality issues are managed for high-value datasets.	Continual improvements of data quality system.
Make Data Safe and Secure	Data is stored in ad-hoc facilities.	Data security facilities and data security standards are being established.	Dataset is held in a system with well-defined data security and storage facilities.	Data routinely managed in secured repositories.	Continual improvements of data security and safety systems

GLOSSARY

DATA	
Administrative data	Information collected for delivering public administration, e.g. for registration, transaction and record-keeping.
Business glossary	Simpler version of data dictionary, defining terms relating to a dataset in ordinary business language clearly understood across directorate (business-facing definitions).
Data	Observations and measurements of things that we are interested and care about. Based on the facts, observations, images, computer program results, recordings, measurements or experiences on which an argument, theory, test or hypothesis, or other activity or output rests. Generated, collected, acquired or used during projects or public service operations, and in some cases may include the output itself. May be numerical (quantitative), descriptive (qualitative), visual or tactile. It may be raw, cleaned or processed, and may be held in any format or media. Evidence of organisation business activities is considered a record.
Data capture	Systematic recording of data. Once captured, organised and evaluated, data becomes information. When data and information are analysed and interpreted in the context of the organisation, the key lines of inquiry or questions, and in relation to other factors and variables, they become evidence.
Data dictionary	Document comprising the technical definitions and metadata information of all fields in a dataset.
Dataset	Structured collection of data, that is stored, published or curated in a single source, available for authorised access or download in one or more formats. Lists values for each of the variables for each member of the dataset. Can consist of a collection of data, documents or files. A dataset in tabular forum includes columns representing a variable and each row corresponding to a given record.
Dataset register	A list of all known datasets to provide visibility, discoverability and access to authorised users. Can be a simple list such as in shareable document, or a SharePoint site or data catalogue.
High-value data	Data that would have a higher economic value if made available as open data due to its authoritativeness, timeliness, accuracy or other traits.
Linked data	Data created from matching and integration of two or more datasets. This may occur through either an explicit match on unique identifiers, or through a combination of information that gives a high confidence match between the datasets.
Master data	Core dataset that is essential to government operations.
Metadata	'Data about data', a set of information or facts about the data in the dataset(s) for the purpose of attribution, description, management, verification and discovery.
Public sector data	Data captured (collected, generated or acquired) by the public service for policy development and public administration. Also known as Public Sector Information.
Quality standards	Set of criteria used to measure data quality.
Records	The International Standard on Records Management (ISO 15489) defines a record as "information created, received, and maintained as evidence and information by an

	organisation or person, in pursuance of legal obligations or in the transaction of business." The *Territory Records Act 2002* draws on the Standard in defining Territory records, which are records made and kept, or received and kept, by a person in the course of exercising a function under a territory law.
Reference data	Sets of values or classification schemas that are referred to by systems, applications, data stores, processes, and reports, as well as by transactional and master records.
Structured data	Organised data that is generated by people, such as when data is inputted into a computer in spreadsheets and databases (e.g. name, age, post code, gender), and by machines such as Sensory Data (GPS data, street sensors, Bluetooth devices, medical devices), Point-of-Sale data (credit card information, product information), call detail records (time of call, caller information) and web server logs (page requests).
Unstructured data	Information that either does not have a pre-defined data model and/or is not organised in a predefined manner. Forms of unstructured data include social media, text files (e.g. word documents, PDF documents, books, letters, other written documents, audio and video transcripts), audio files (e.g. customer service recordings, voicemails), presentations (e.g. PowerPoint), videos (CCTV, personal video, YouTube), images (e.g. photographs, illustrations, memes), messaging (e.g. instant messages, text messages).
DATA USERS	
Authorised user	Someone assessed by a data custodian, including through the application of the Five Safes data sharing principles, as being authorised to access and use data for an agreed and authorised purpose, especially data that may include personal, confidential and/or sensitive information.
Data custodian	Typically a senior executive or manager, accountable for data governance decisions for all internal and external datasets assigned to them.
Data owner (also known as data provider)	Individual, household, business or other entity that provides data to a government agency or has data about them supplied by a third party
Data steward	An officer or manager responsible for operational data management and decisions for all internal and external datasets assigned to them.
DATA SHARING AND OPEN DATA	
Data release	Making data publicly available with no or few restrictions on who may access the data and what they may do with it.
Data sharing	Making information or data "available to another agency, organisation or person under agreed conditions." When we share data, we are clear about who it is shared with and why, and the specific conditions, controls, and safeguards under which it is shared.
Data sharing agreement	A formal arrangement between a data custodian and another agency, organisation or individual that details conditions under which data is shared and used.
Open access	Provision of free and unrestricted access to information to the general public.
Open data	Publicly available data that can be freely used, reused and redistributed by anyone without restriction.
DATA SAFETY AND SECURITY	

Data protections	Changes made to data to minimise the likelihood of identifying the Data Provider.
De-identified data	Data relating to a specific individual where personally identifying details and unique characteristics have been removed to prevent identification of that individual. Also known as anonymised data.
Non-sensitive data	Data that is anonymised and does not identify an individual or breach privacy or security requirements.
Personal information	Also known as personally identifiable information or PII, this Framework uses 'personal information'. The *Information Privacy Act 2014* defines personal information as "information or an opinion about an identified individual, or an individual who is reasonably identifiable— (i) whether the information or opinion is true or not; and (ii) whether the information or opinion is recorded in a material form or not; but (b) does not include personal health information about the individual."
Sensitive information or data	The Office of the Australian Information Commissioner defines Sensitive Information as a subset of personal information, or an opinion (that is also personal information) about an individual's: racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information about an individual, genetic information (that is not otherwise health information), biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or biometric templates. Other forms of sensitive data can include confidential data such as commercial in confidence information and research data, and ecological data that may place vulnerable species at risk. The Office of the National Data Commissioner identifies *Particularly Sensitive Data* as any data where unauthorised disclosure would likely lead to adverse consequences for the individual, agency, organisation or Australia in general. Data which is of a personal, legal, commercial, security or environmental nature may be considered particularly sensitive. This is broader than the *Privacy Act 1988* definition of sensitive data which is defined as a subset of personal information and limits how it can be collected and used.

APPENDICES

- ☐ Appendix I Developing data-driven, evidence-based policies and practice
- ☐ Appendix II Developing a directorate data strategy and roadmap
- ☐ Appendix III Five areas to enable and improve safe data sharing
- ☐ Appendix IV Foundational principles of privacy by design
- ☐ Appendix V Lead data roles and responsibilities

Appendix I
Developing data-driven, evidence-based policies and practice

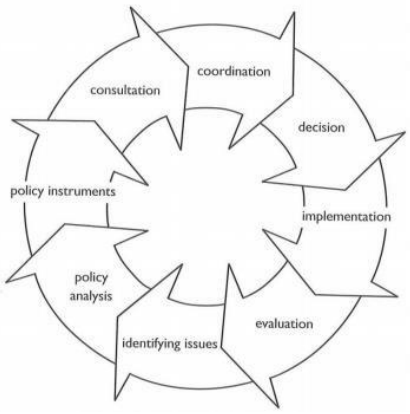
By bringing together different kinds of data and evidence from multiple sources and using it in a conscientious, explicit, and judicious way, we build up a picture of what happened, why it happened, and the probability of what caused it and what else may happen.

We are not without frameworks, guides, user manuals and tools to "do" evidence-based policy. In 2003, Peter Bridgman and Glyn Davis wrote "What use is a policy cycle? Plenty, if the aim is to help public servants make sense of the policy task. Setting out a sequence of steps to turn ideas into Cabinet recommendations can provide structure in the otherwise dizzying world of policymaking. It would be a mistake, though, to see a policy cycle as other than a first step, a guide amid complexity. To read the policy cycle as rationalism revived is to misjudge both form and intent."

They espoused the first principles of evidence-based policymaking as:

1. Building and compiling rigorous evidence about what works and doesn't work, including costs and benefits.
2. Measuring effectiveness through monitoring and evaluating impact.
3. Using rigorous evidence to improve policy implementation, scale what works, and redirect funds away from consistently ineffective programs.
4. Encouraging innovation and test new approaches.

Later along with Catherine Althaus, Bridgman and Davis delivered an eight-step policy cycle in *The Australian Policy Handbook* now in its 6th edition.



1. Issue identification 2. Policy analysis 3. Policy instrument development 4. Consultation (which permeates the entire process) 5. Coordination 6. Decision 7. Implementation 8. Evaluation

The process helps us to **know** the problem, why it exists and persists, who is impacted and needs to be involved to better understand the problem and collaborative with to (co)design the policies and interventions, and how we might change it such as by using pragmatic approaches for successful implementation and impact.

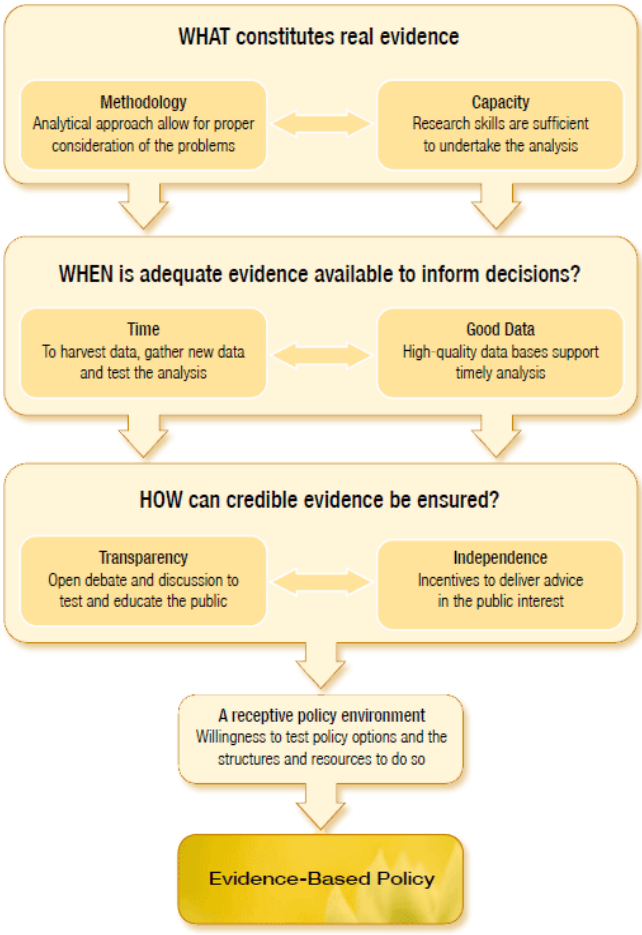
Gary Banks AO in 2009 also wrote about the **essential ingredients for evidence** that help us to discharge government functions by using the right evidence, at the right time and to be seen by the right people. Doing evidence-based policy "takes time and effort of many not a few".

Banks asks three questions for using data and evidence in policy decisions: WHAT, WHEN, HOW.

WHAT constitutes real evidence are: Methodology – Analytical approach allow for proper consideration of the problem and **Capacity** – People skills are enough to undertake the analysis.

Methodology: The analytical approach chosen must allow for a proper consideration and understanding of the problem: what are questions we need to answer, what is the nature of the issue or problem and what are the different options for policy action. To Banks, failure to do so is one of the most common causes of policy failure and poor regulation. Further, Banks argues for the need to measure the policy impacts using range of methodologies available. However, this invariably depends on the topic and the task at hand, ie whether the assessment will be ex-ante or ex-post.

Capacity and Culture: By attracting, retaining and boosting our people skilled in quantitative and qualitative methods and other analytical approaches in the public service, we can take a more data-driven and evidence-based approach. Our people need to work with data and conduct research, reviews and evaluations. It our people who will foster organisational cultures of data- and evidence-based decisions.



WHEN is adequate evidence available to inform decisions? Time – To harvest data, gather new data and test the analysis and **Good data** – High-quality databases support timely analysis

An essential ingredient in evidence-based policy making is **data**. National institutions such as the Australian Bureau of Statistics generates data assets that can be used widely. However, the public sector must capture, share, use and reuse data from other sources such as administrative collections, policy reviews and evaluations. To so, will ensure we genuinely begin to realise the real value of data for good policy.

HOW can credible evidence be ensured? Transparency – Open debate and discussion to test and educate the public and **Independence** – Incentives to deliver advice in the public interest

Transparency means to honestly and openly disclose the innerworkings of data, assumptions and methodologies used, "such that the analysis could be replicated". The independence of technical research can enhance the potential for gaining robust and unbiased evidence to inform policymaking.

Use more inclusive and open methods afforded to us by design thinking and systems approaches, as these provide a useful and necessary source of good evidence to support policymaking.

As well as consulting with experts, seek the reactions and feedback from the people who are likely to be *affected* by the policy, to provide insights into the likely impacts and help avoid unintended consequences. Banks says, the wider the policy impact, the wider the consultation process should be. This affords government with the level of transparency in policymaking and enabling us to understand community reactions to unformed policy ideas and to better anticipate the potential of success of the different options.

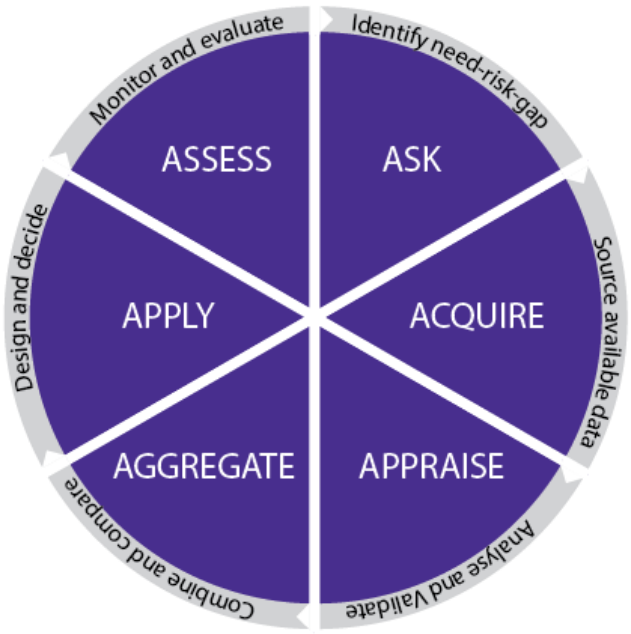
Moving away from green paper-white paper processes, the data and evidence gathered and used during codesign and coproduction, research and evaluative approaches can provide government with a greater potential for meeting community need.

Finally, the public service needs to make greater use of detailed and independent research and consultations, involving time spent to gather data and test the evidence. Where the necessary data is not available, that the public service needs to consider how it will acquire it such as through special collections using surveys or by conducting programme evaluations and pilot studies or trials. Banks notes the imperative to have a **receptive policy environment** with the willingness of all stakeholders to test policy options and the structures and provide the resources to do so.

Steps to conduct data-driven and evidence-based policy and practice

Bringing this together, the guide below five steps for data-driven and evidence-based policy and practice:

1 **Ask** the right questions to identify need and demand for the topic
Understand the topic and determine what question is being asked.
Continually review and assess the analytical steps to maintain focus on the goal or objective of the project.



2 **Acquire** the right data and choosing the right analytical method
Use the most appropriate data for answering the project questions.
Assess the quality of the dataset, to ensure reliability and accuracy.
Use a standards-based, or in some cases standardised, approach to defining the right dataset: e.g. common platforms or data points allow us to "compare like with like".

3 **Appraise,** analyse and validate, **aggregate**, combine and compare data to inform the design of policy and practice options.
Set expectations of the data and quality check during analysis.
Drill down into the data. Look at what may be underlying the results.
Data flow and analysis should be iterative (not linear): i.e. check the process for robustness, validity and reliability at multiple points.
Determine whether the story is being supported by the data.
Determine if the story answers the questions proposed at Step 1.

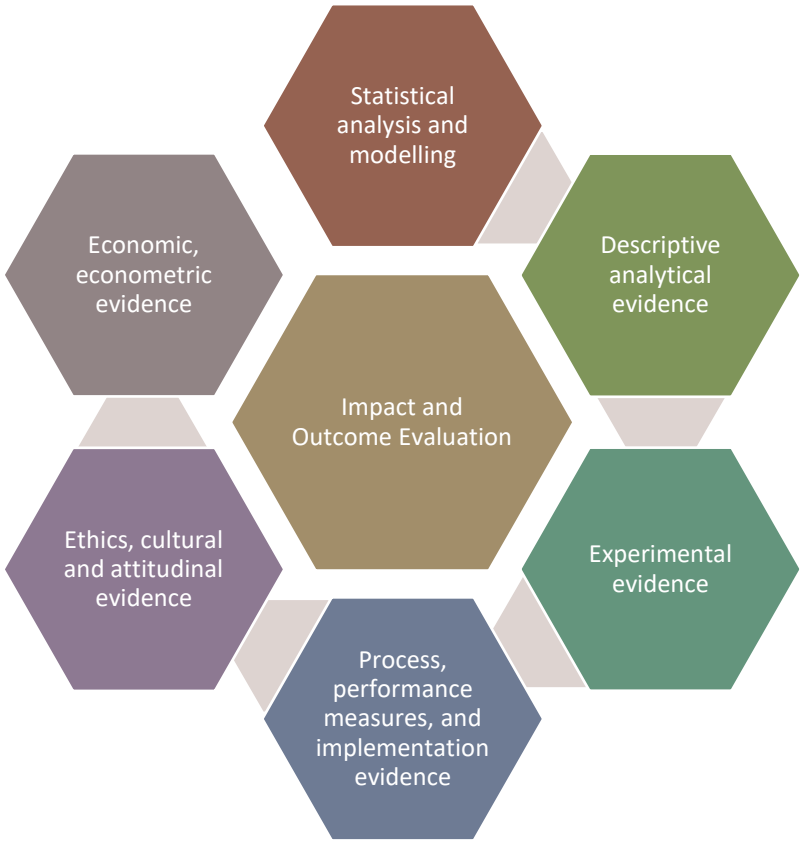
4 **Apply** the insights and knowledge in practice while continuously **assessing** progress, monitoring and evaluating outcomes and communicate and share these with stakeholders
The message should be clearly conveyed in plain, easy to understand language.
Well-designed graphs are a great way to visualise the data and clearly explain the story, as well as facilitate additional analysis and interpretation.
Report the data processing and analysis methods used, in addition to the data itself.
Factor in time for quality assurance.

5 **Update** the Knowledge Base
The evidence we now have forms part of the knowledge base. Depending on sensitivity and ethical considerations, it should be shared.
By internally and/or externally publishing the data, the techniques used, and the analysis and interpretation, we can provide other colleagues and broader community the opportunity to both review the data and use it in future research, policy and program design.
Strengthen our knowledge, build strong networks, and keep up-to-date on our understanding of matters related to our work and priorities.

Types of data used in policy and practice

An enormous amount of qualitative and quantitative data is available from multiple sources and locations such as on our administrative systems, other Government databases, online resources and printed materials. We source them for a range of purposes to make evidence-based decisions. The following figure lists the different types of evidence that are used by the Organisation.

Examples of data and evidence sources



Knowledge and evidence-base according to their source and method:

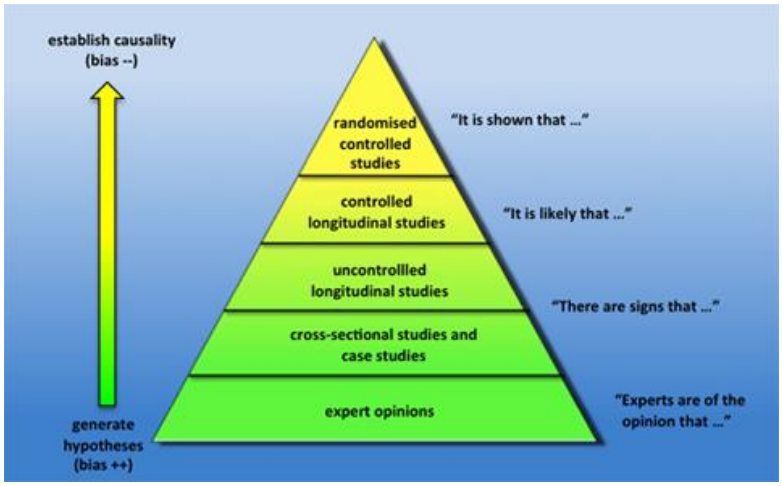
Research	Scientific, research and rigorous knowledge and subject matter expertise: research theories, synthesis, strategic and applied scientific inquiry, single/mixed methods, economic and financial modelling
Professional-managerial experience	Practical, technical service and clinical knowledge, experience and expertise, professional networks, mixed method, pilots/trials, randomised controlled trials, quasi-experimental studies, economic and financial modelling
People – service users, customers, clients and patients, communities and stakeholders	Individuals, families, carers – their lived experiences, personal knowledge, meanings, motives, stories and narratives, context, goals and interests, values, attitudes, perceptions
Service system context and environment	Strategic, tactical, national, and regional knowledge, systems knowledge, experience and expertise, political knowledge, mass media, economy, priorities/approaches, policy, audits, planning, quality, performance, outcome and evaluation activity

Importance of quality and levels of information and evidence

As identified above, we use a range of data and information from various sources and in varying formats. While it is good practice to ensure that policy and practice decisions are made using a mix of evidence types and from a range of sources, it is particularly important to ensure the evidence we use is relevant, appropriate, accurate, valid and reliable. The challenge remains for data users and decision makers is how to ensure that the evidence used is robust and reliable, i.e. that it can be trusted.

However, not all data and evidence are created equal. While we build our capabilities and understanding of using data, insights and evidence in our work, we also need to improve our capacity to interpret data and evidence to inform decisions. We need to understand the limitations and benefits of using data and analytical processes, and as such to collectively understand the quality and different levels of evidence.

In health and medical research, there is a relatively widely accepted concept of a "hierarchy of evidence", by which evidence is ranked according to a set of methodological criteria. Several organisations have designed different hierarchies or approaches for assessing the available evidence. These include the National Health and Medical Research Council (NHMRC), the Centre for Evidence-Based Management (CEBMa), and UK's Oxford Centre for Evidence-Based Medicine (CEBM). Hierarchies or levels of evidence designed for use by researchers and evidence creators and users to support greater understanding or the strength, quality and efficacy of scientific research.



Generally, the hierarchy classifies evidence ranging from random assignment studies (randomised controlled trials) as the strongest level of evidence, followed by evidence from quasi-experimental designs, studies relying on a selection of observed variables and before-after comparisons, and finally, evidence based on opinions of experts and authorities and descriptive studies at the lowest level on an evidence hierarchy.

The designing of such 'levels of evidence' recognises the importance of methodological design to the research question – essentially the higher the level, the better the quality. 'Levels of evidence' are ascribed reflecting the risk of bias in the research design; "the quality of the study and the likelihood that the results have been affected by bias during its conduct; the consistency of its findings to those from other studies; the clinical impact of its results; the generalisability of the results to the population for whom the guideline is intended; and the applicability of the results to the Australian (and/or local) health care setting". (NHMRC 2009: 2)

In summary, to ensure we use the best available and robust evidence we need to be aware of the quality issues inherent in the evidence we are working with. There are two main dimensions that should be considered: (i) **the quality of the data**, and (ii) the **methodological framework** used to collect, produce and analyse the data.

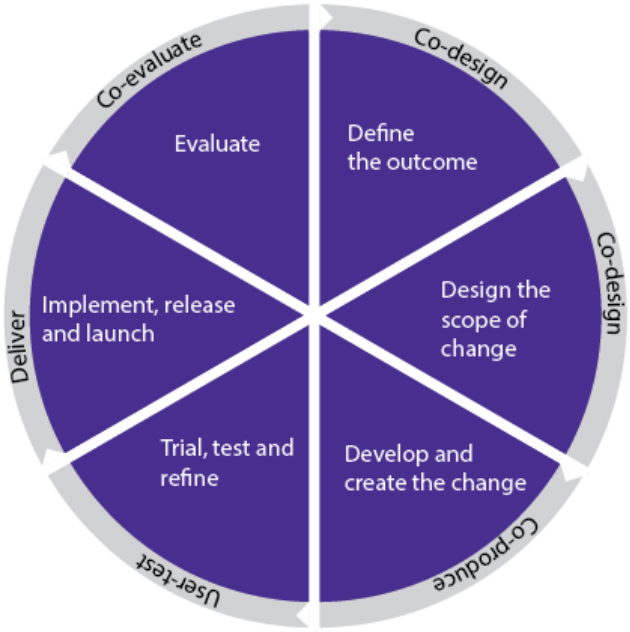
Some principles to keep in mind are to:

- use a range of the available high-quality evidence rather than relying on a single study;
- be aware of the quality variations manifest in most datasets;
- be aware and assess the quality of the methodological approach (was the data collection and management method rigorous, valid, reliable, objective, protecting individual privacy); and
- where data is lacking or unavailable, it is imperative to consider data collection method and systems meet requirements set out in data quality frameworks.

ACT Government Design Wheel

Another framework that governments are using is design thinking and systems-based design. The ACT Government Design Wheel learns from design thinking and agile methodologies, and applies the central elements of policy and project cycles:

- Issues Identification
- Analysis & Options Development
- Consultation
- 'Political' Decision
- Implementation
- Evaluation



The design wheel is a useful conceptual tool for policy and program development, providing guidance on what each stage of the cycle should include. There is a data dimension to all aspects of policy and program design. For example, what evidence is informing decisions? Who does the information you use belong to and who manages it? What steps are you taking to ensure privacy and security? What data can you share or can be shared with you to deliver better outcomes?

Design Wheel Section	Key messages
Define the outcome	• Understand the key purpose and determine what question is being asked. • Continually review and assess the analytical steps to ensure you maintain focus on the goal or objective of the project. • Ask: how might you measure the outcome, and what data is needed?
Design the change	• Set expectations during the design stage for data collection, sourcing, handling, use and sharing. • Ask: what is the data model, master and reference data, data quality standards, data system, data source and storage, and data provenance?
Develop, create the change	• Ensure data design embeds the ACT Data Governance and Management principles to ensure data is fit for purpose, reliable and accurate (quality-in, quality-out). • Use data standards to define the right data at the outset of data acquisition or development. • Develop: metadata and data profiles.
Trial, test and refine	• Set and check expectations of the dataset, trusted data flows, and quality during trial, test and refine stage. • Ask: does the data meet data quality standards and master data requirements?
Implement, release and launch	• Ensure continuous monitoring and improvement of data practice including privacy and security. • Review: data models and data provenance.
Evaluate	• Determine whether the story (operational, tactical or strategic level analysis) is being supported by the data. Having an expectation of what stories are likely to be told, is a good way to help check the quality of the data early. • Ensure the message is clearly conveyed in plain, easy to understand language and data visualisation. • Review: data profile and quality over time.

Resources

to support us to learn more about using data in our work

- The ACT Government's Design Wheel
- The steps informing evidence-based policy
    - Banks, G., AO "Challenges of evidence-based policy-making" (2009 – Archived) https://www.apsc.gov.au/challenges-evidence-based-policy-making accessed on 21 June 2020
    - Althaus, C., Bridgman, P., and Davis, G., (2017) *The Australian Policy Handbook: A Practical Guide to the Policy-Making Process* (6th Edition). Sydney: Allen & Unwin.
- Cochrane Collaboration, http://www.cochrane.org – for medical research findings to facilitate evidence-based choices about health interventions
- Campbell collaboration, https://campbellcollaboration.org/ – for evidence syntheses such as systematic reviews of the effects of social interventions.

Appendix II
Developing a directorate data governance and management implementation strategy and roadmap

Directorate strategies to implement this framework and guide must be centred around understanding why and how using data better will help, how data is being used now, and what is the gap.

Typical tasks to develop a strategy include:

- Assess the current state and context (use PESTLE analysis[23])
  - Who are our beneficiaries? Customer context and service environment
  - What is our mandate and legal role? Legislative and Policy environment
  - What is our funding model? Funding and investment context
  - How do we operate? Our business model and operating environment
  - What works, what is our impact? Performance and outcomes analytical model
- Establish a set of Strategy Design Principles
  To derive value, the strategy must acknowledge the core barriers to take action and leverage the opportunities available
- Design vision, mission, purpose, objectives - that will
  - Vision, Mission and Purpose: A clear view of our future; a compelling case for change; re-energises the organisation and staff to strive to achieve an explicit purpose
  - A statement of need for the organisation and target beneficiaries
  - Match our hopes for the future
  - Help motivate our staff
  - Drive our culture
  - Be used to communicate consistently with our customers and partners
- Engage stakeholders from the beginning and across our ecosystem
  - Actively hear from internal and external stakeholders – be outcomes focussed
  - What are their goals, hopes, fears, What's In It For Me (WIFM), what's in it for everyone
  - Customers, service users, clients
  - Staff and executives
  - External agencies and partners
- Use the information and insights to explore
  - what needs to be continued, as it is working well
  - what needs to be changed and stopped
  - what new opportunities and innovations we need explore

[23] PESTLE stands for Political, Economic, Social, Technological, Legal and Environment. For further information, see https://pestleanalysis.com/what-is-pestle-analysis/.

What to include in a Data Strategy?

The following outlines the structures, sections and content you will need to include in our strategy.

Why	Our reason for being, purpose, cause or belief – our hopes for the future A clear view of our future; a compelling case for change; re-energises the organisation and staff to strive to achieve an explicit purpose
Our vision:	A sharp enduring vision statement defining our cause and what we believe in?
Our context:	Our drivers, environment, and core public sector values
Our current state:	Our strengths, weaknesses, pain points, what customers think, and case for change
How	How will we give life to our vision and cause – our everyday Define the Strategy Design Principles To derive value, the strategy must acknowledge the core barriers to take action and leverage the opportunities available
Our mission:	A simple statement defining our purpose and core focus – what we do to make our vision a reality
Our customers:	A simple statement defining our customers and key stakeholders
Our culture:	A set of values, behaviours, and principles that give life to our mission
What	What we will do to achieve our Why? The things we create, our products and services Establish an outcome-based Strategy along the lines of 1. Capable, Empowered People & Culture 2. Enabling Processes & Systems 3. Investing for success 4. Accountable Governance and Policies
Our objectives:	*Our priorities, products and services*: what we are here to do and what we will pursue incl ongoing work *Our Accountability*: our leadership and governance mechanisms focussing on decision and accountability *Our People and Culture*: our learning and development opportunities focussing on workforce, values, and behaviours Our Systems: our control, coordination and management systems and investment model *Our Work*: our operational processes includes how we work, our supply chain across a broad ecosystem, staff roles and responsibilities
Our way of working:	How we will organise ourselves and apply our resources, skills, capabilities, and know-how to achieve our mission and objectives
How well	Describe what does success means and when will we know we got there?
Our outcomes and impact:	Our success factors defined by what difference we make for DIIS, and other stakeholders incl efficiency and effectiveness measures, can we define a program logic / outcomes map
Implementation	When we deliver on our promises? Making it happen with great execution powered by change leaders who are agile, lean, design thinkers, user-centred, outcomes-focussed
Our Roadmap:	A sequence of strategy outputs and anticipated outcomes – use Continue, Start, Explore model
Maturity model:	A measure for assessing the data governance and management steps across five levels of maturity: Initiate; Develop; Define; Manage; Optimise.

How to develop a Data Strategy?

A key first step will be to discover why data is important to our directorate and how it will benefit our customers, partners and the community – ie how it aligns to achieving our directorate strategies, goals, and priorities. Consult far and wide, identify which areas are well placed to remedy data culture and practice challenges and barriers. This will help us uncover both the current state and future state of making our organisations more data-driven, by improving our data governance and management practice.

Examples of engaging and consulting widely include holding a series of conversations with internal and external stakeholders at all levels. Take a formal or informal approach or both. Join existing forums, groups, formal governance groups, and team meetings. Set up focus groups and deliver surveys. Establish and open and digital chat channel on the directorate intranet site or deliver whiteboards on each floor for staff to share their thoughts.

Develop a what we learned, or what we heard summary. Use this to learn about the key pressure points and challenges people face in using data, their interest and importantly their readiness and barriers to using data, and give us insights to help shape the structure and contents of the strategy and implementation roadmap.

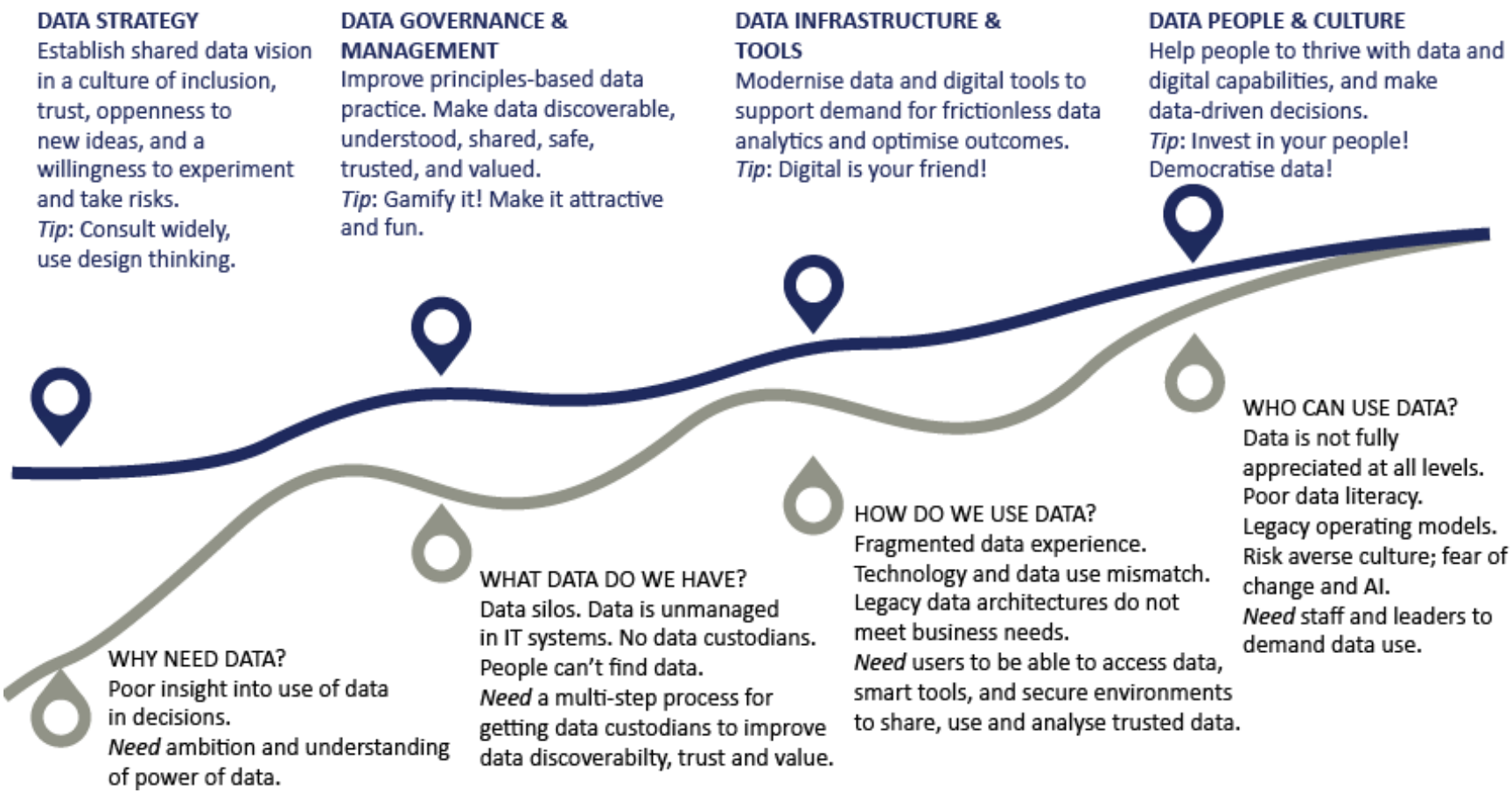
From this information, we can define data strategy elements. Workshop with internal and external directorate stakeholders, the ACT data vision and data governance and management principles.

- Vision: establish an inspiring and shared vision provides us with a compelling "why“ ie our deep-seated purpose, our cause, our hopes for the future and what difference we want to make as a division. It can drive our culture and help us to communicate our why. This is what inspires us all to wake up and come to work and, then at the end of the day, we go home feeling fulfilled by the work we do.
- Mission and objective: establish the core change mission that will help us bring our vision to life to support customers and signals how we will work – this is our everyday.
- Confirm and refine:
  - why data is important to achieve strategies, goals, decisions, customer and community need
  - what is their reason for being
  - why and how using data better will help them
  - what is the current-state - how data is being used now, what are present attitudes behaviours towards data – what is the existing cultural norms around data and data use?
  - what is the gap between the desired state and current state? What are the barriers and what must be true and present to enable change?
- This will provide insights to shape the strategy and roadmap structure and content consider
  - Capabilities across people and culture, governance and policy, process and practice, and technology, systems and tools
  - Implementation needs and risks eg funding, cultural barriers, executive buy-in
  - What success will look like and how will we measure progress
  - Develop a change map or blueprint for change – what is needed to help generate, share and apply quality data and evidence in our policy, programs, services and operational decisions.

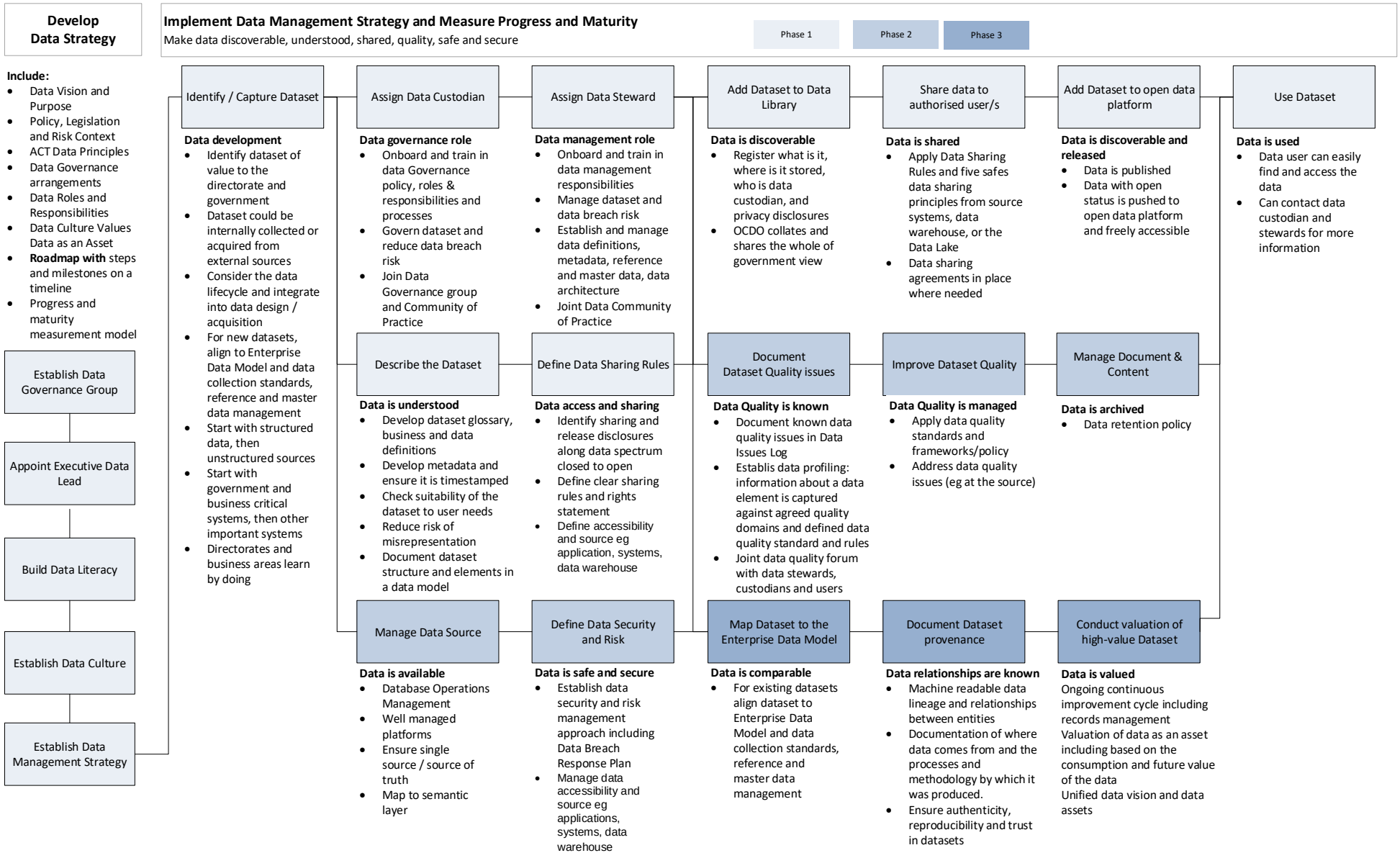
As at 2020 Our Current State	Change Actions between 2020 and 2022	By 2022 Our Desired State
Identify themes and capabilities across people and culture, policy and governance, process and practice, and technology, systems and tools	Implementation needs and risks eg funding, cultural barriers, executive buy-in What needs to be true and present to make the change across strategic, tactical and operational levels	What success will look like and how will we measure progress – ie the future desired change including cultural norms and practice

- Strategy priority areas
  - Governance and policy:
    - Data committees
    - Data Governance and Management framework / roadmap
  - People and culture:
    - Data roles and responsibilities
    - Data analytical and data story telling capabilities, training and development
    - Executive data needs
    - Data culture activities – culture hacks, communication
  - Process and Practices
    - Data analytics for our business?
      - what are the key questions we need to answer to achieve priorities, customer satisfaction
      - Use cases showing insights-informed decision and outcomes using data analytics approaches
    - Data analytics framework – how to
  - Data systems and tools
    - Data analytics infrastructure (data lake, data warehouse)
    - Data analytics and visualisation tools (SAS, SPSS, PowerBi, Tableau, ESRI ArcGIS)
- Communicate and Change: We will share our vision regularly with our division, customers and other stakeholders. Our Strategy will provide a clear set of measures which we will take to achieve our vision and mission. We will have ongoing communications of stories of progress and change.

A proposed journey to build data governance and management maturity to maximise the value of ACT Government data assets through use, reuse and sharing



Sample order and phases to help simplify and gamify how we bring our datasets under good data governance and management over time



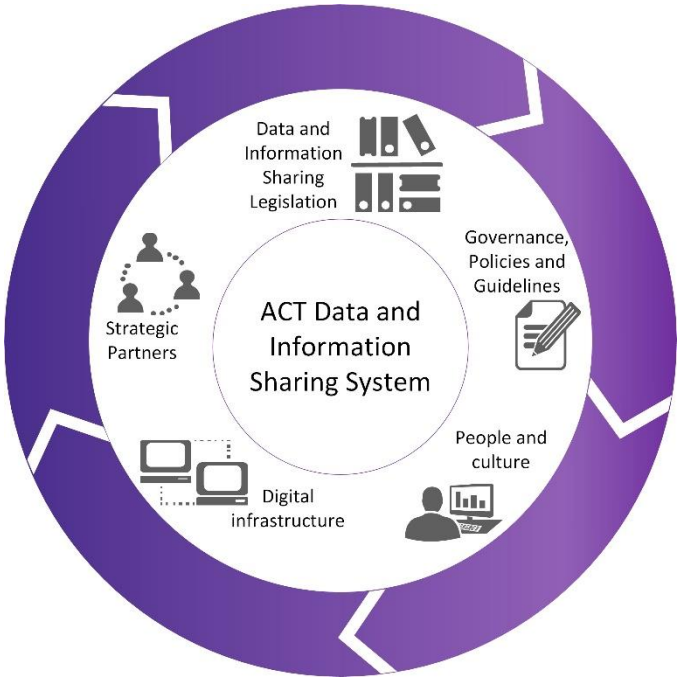
Examples of tools, capabilities and resources that can help bring our datasets under good data governance and management over time

	Data Acquisition	Data Collection	Data Quality	Data Modelling	Data Protection	Data Sharing and Release	Data Management training	Data Community of Practice
Why	Staff need access to internal and external data to inform their decisions. Staff need to also make curated, trusted, and reliable datasets available through central data location.	Gathering information and observations on areas of interest enables us to deliver programs, support policy design, answer research questions, and evaluate outcomes. Staff need help to ensure the data we collect is comparable, consistent, and trusted for use.	Ensuring the quality in the data we use is necessary to drive trust in the decisions we make from the data insights. Staff need support to employ a consistent data quality process to manage data risks.	A data model is a representation of the world we observe with information about it. It helps us to ensure required data objects can accurately support the business needs. Staff need help to build data models as a blueprint for designing and delivering data collection mechanisms and systems to support operational management.	We take a proactive approach to ensuring the privacy and protection of our data holdings and use. Staff need help to build privacy into the design, operation, and management of our data systems and processes including to ensure safe and trusted data use, sharing and release.	Releasing and publishing of data to organisations and the broader community can support innovations and value creation. Staff need support to deliver the government's open data policy for greater wider value creation through data release, while balancing release of data with privacy concerns.	Well-managed, high-quality data is integral to answering complex business questions in a timely manner. Program and policy staff, and research teams are responsible for the management, quality and stewardship of data we hold.	Data users, custodians and stewards responsible for use, governance and management of data, support each other in a community to improve their knowledge, keep up to date on practice, and impact on good data governance and management.
How	• Identify staff data needs • Assess source and availability of data • Assist in acquiring the data safely storing and sharing data (internally). • If required, manage data licensing and governance.	• Define and understand your data needs across the data lifecycle • Match data needs to the data standards • Support the design of data collection in a standard way.	• `Support Data Stewards to ensure data quality across the data lifecycle, from initiation to reporting. • Apply the Data Quality Toolkit to guide and improve data quality. • Establish and manage data quality group.	• Provide advice on data modelling to suit business needs such as in program design. • Develop data model using best practice. • Provide access to existing data models. • Develop Enterprise Data Model.	• Define staff responsibilities and obligations when working with data. • Develop data incident response plan • Manage disclosure risk • Build acceptance, demonstrate value and trust in how we use data.	• Define high value datasets for open release. • Support data stewards to place data on the open data platform • Build acceptance, demonstrate value and trust in how we use data.	• A course for data custodians, data stewards and other staff to be gain knowledge and improve their practice in data management, governance and use.	• Meet to discuss, share, and learn about work • Data Specialists support the administration and management of the Community of Practice including maintain of the memberships.
What Product/ service	• More number of datasets available through central data location.	• The Enterprise Data Model • *Support the linkages* with *Data Quality Toolkit*	• Data Quality Toolkit. • Data Quality metrics. • Data Quality Group	• Enterprise Data Model as a single source of truth for all (common) the business level data. • Master data management • Data models for each ICT System software used to support business operations	• Privacy and trust principles • Five Safes Framework • Data incident response manual • Social Licence and Privacy Impact Assessments • Data security • Data sharing advice	• More data released and made open and available on data.gov.au • Data release advice incl disclosure or publication Govhack support • Data sharing rules	• DAMA DMBOK certification or in-house training course • *Applies the Data* Governance *and Management Framework* • *Associated with Data Community of Practice*	• Quarterly Data Community of Practice meetings. • Workshops, presentations, and masterclasses arranged on key topics from time to time

	Data Acquisition	Data Collection	Data Quality	Data Modelling	Data Protection	Data Sharing and Release	Data Management training	Data Community of Practice
Outcomes	Staff can access and use more data in their day to day operations.	Staff achieve accurate and honest collections using established systematic processes and systems.	Staff can trust the data they access and use. Data can be treated as an asset to and can be trusted, to harness its power to deliver insights and our core mission.	Data is shareable, consistent, and re/usable. Improved communication between data stewards, data custodians (ICT staff), and other staff.	Safe and trusted use, sharing and release of data Data privacy is protected, and social licence is managed	Quality and trusted open data for public access or use by third parties Enabled wider value creation from use of our data such as to support business innovation and growth.	Increase data literacy, well managed and trusted data sets, engaged and enabled staff, data first culture.	Increase data literacy, well managed and trusted data sets, engaged and enabled staff, data first culture
Goals	Enabling the acquiring, storage, sharing and use of data to make effective evidence-based decisions and impact, conduct research and improve operational efficiency and effectiveness. Releasing data on the open data platform to enable broader use. Supporting data users, custodians, stewards, and decision makers to be able to make quality, trusted and curated data readily accessible for wide and safe use Taking a proactive approach to ensuring the privacy and protection of data holdings and use. Building privacy into the design, operation, and management of data systems and processes. Supporting data users, custodians, stewards, and decision makers to know their responsibilities and obligations when working with data Ensure safe and trusted data use, sharing and release Ensuring data protections and management enable social licence to be managed and maintained.				Developing peoples' data governance and management capabilities helps to equip and empower them to make appropriate decisions and choices in data practice.			

Appendix III
Five areas to enable and improve safe data sharing

ACT Government Directorates are improving how staff use public sector data to deliver benefits for Canberrans through better policy and programs, improved research opportunities, and person-centred and streamlined government service delivery. On 4 September 2019, the Strategic Board agreed to enhance ACT Public Sector data and information sharing. The Strategic Board approved the five priorities to enable the ACTPS to share our data in safe and trusted ways. As a package, these form a simple data and information sharing framework and span areas such as the building data capabilities and skills, establishing data management processes, investing in data systems and infrastructure and embedding a data and digital first culture that will enable data sharing, integration, and release.



We have learned from past good efforts by the ACTPS to share data and information, that then encountered systemic, operational, and cultural barriers (which impede progress). These five areas will provide opportunities for the ACTPS to share and use data, while maintaining the strong security and privacy protections expected by the community.

1. Data and information sharing legislation

Review, identify and understand any privacy, secrecy and confidentiality provisions that exist within legislative frameworks, as well as any considerations around third party data ownership.

When considering the legislation that may guide, prevent or restrict data sharing for each directorate or agency, it is important to spend time to consider what authorisation and framework can assist it is necessary to satisfy applicable regulatory restrictions on sharing. However, there may be an opportunity to consider additional controls that can support the sharing of data, rather than being a barrier to sharing. All staff should have a sound understanding of the limits of what they can share under the relevant legislation, rather trying to establish what is and isn't permissible on a case by case basis.

Data custodians can establish clear and consistent advice for data sharing requests by data users around why and how data can or cannot be shared. For example, if data cannot be shared in its raw form due to a legislative provision, the data custodian can identify solutions to make the data shareable, through applying risk and data treatment methods such as de-identification or aggregation that enable safe sharing.

It is acknowledged that in the ACT there are several primary laws that govern the capture, sharing and use of data and information between authorised entities. The ACT Government is learning from the experiences of other Australian jurisdictions where overarching legislation supports greater levels of data sharing.

2. Develop strong governance, policies and guidelines

Review and establish the right authorising environment to enable information and data sharing, including the development of review and check points within directorates.

Establish directorate-level data sharing frameworks with supporting policies and strategies to operationalise them. The ONDC's best practice guide for applying data sharing principles provides detailed

guidance on using the five safes principles to share data in safe and trusted ways. In the ACT, directorates may already have their own mechanisms enabling them to share data, including agency specific frameworks, processes, systems and tools.

By applying whole of Government data governance and data management principles as well as the Five Safes data sharing principles, all directorates can improve consistency and comparability in data sharing arrangements across the ACT public service, as one government.

Another key tool for safe and effective data sharing is to establish **data sharing agreements** between a data custodian and the organisation receiving their dataset. Using the five safes data sharing principles, these agreements provide the data custodian with the necessary information to satisfy a range of requirements including the purpose and uses of the data, and details of data use activity. Data custodians can gain confidence and reassurance that data users have established good data governance and risk mitigation mechanism for the shared data. It is best practice to make data sharing agreements publicly available to maximise transparency, including through establishing and publishing a register of existing agreements.

Data Sharing Agreements usually contain the following elements:

- Parties to the agreement
- Purpose - what the data can and can't be used for
- Duration
- Information to show the data sharing agreement adheres to the Five Safes Principles
    - Project: is the data being used for an appropriate purpose that delivers public benefit?
    - People: do the people using the data have a 'need to know'?
    - Setting: does the access environment prevent unauthorised use or disclosure?
    - Data: has appropriate protection been applied to the data?
    - Outputs: is the output from the data sharing arrangement appropriately safeguarded before any further sharing or release?
- The agreement should also provide information on any sanction that may be imposed if the terms and conditions of the agreement are not adhered to.

The ACT Government will establish a data sharing agreement template to accompany this Framework. A detailed sample template can also be found on the website of the Office of the National Data Commissioner.

3. Establish a strong data culture

Data executive leads, data custodians, all directorate executives and staff are responsible for establishing a strong data culture in their directorates. This includes building the literacy of individuals to recognise data as an asset and promote ideas about how data can support better decision making. Senior executives will drive effective change management processes to break down cultural barriers. All staff are responsible for establishing their own learning and development journeys in order to feel more enabled and empowered to work with data in their roles.

4. Develop digital infrastructure that supports the safe sharing of data

With technological advancements and an appetite for change, there is no better time to address barriers to data sharing within directorates and across government. Directorate information and technology and lead data executives are responsible for enhancing and building new technology that applies a 'data- and privacy-by-design' approach so that digital systems available to staff enable safe sharing based on permissions and in accordance with legislation, governance and policies.

Historically, staff report not being able to access the data they need, when they need it, and in some instances, new or complex digital platforms can add further barriers to data sharing. With legacy digital systems hampering safe sharing and no mechanism for system to system interfaces, when data is shared, it

is often manually extracted, cleansed and shared through outdated and unsecure mechanisms. This limitation leads to risk averse approaches to sharing.

Directorate executives, with data custodians and data stewards, can support capability development through training and work with internal and external partners to ensure our systems are fit for purpose, accessible and enable safe data sharing by default.

The ACT Digital Strategy signals the ACT's intent to create the digital infrastructure to improve digital service delivery and transform foundational infrastructure. It articulates three main dimensions: Growing the Digital Economy; Delivering Digital Services; and Building Digital Foundations. Data sharing is a key product of *Building Digital Foundations*, where establishing appropriate and contemporary data and digital infrastructure can better enable the ACT Government to share identifiable information safely and efficiently, link datasets, draw information from existing systems to create a single view of a client and provide a space for researchers to use ACT Government data assets for research development in a safe and protected way. As such, all government chief information officers, Shared Services and the Office of the Chief Digital Officer are working towards improving our data and digital infrastructure to better service the ACT public service and community.

5. Build strategic partnerships

Build strong strategic partnerships internally and externally to government to leverage the lessons, experiences, skills and knowledge of other organisations or jurisdictions.

The ACT Government already has a range of existing strategic partnerships with stakeholders who provide strategic value, mutual benefit and share lessons, including with other jurisdictions, service providers, not-for-profit and private sectors, and research bodies and academic institutions.

Directorate executives, data executive lead and all leaders including data custodians are responsible for identifying, establishing and building on these relationships and partnerships in progressing their data sharing journeys. Each partnership can provide unique arrangements and mechanisms to yield mutual benefit such as to solve complex policy or service delivery challenges, identify common service needs and vulnerable cohorts, and build community trust and expectations.

Appendix IV
Foundational principles of privacy by design

The Office of the Australian Information Commissioner (OAIC) refers to privacy by design as "manag(ing) personal information in an open and transparent way, (including) taking reasonable steps to implement practices, procedures and systems that will ensure compliance with the Australian Privacy Principles." The OAIC notes that "privacy should be incorporated into your business planning, staff training, priorities, project objectives and design processes."[24]

Privacy by design is a concept first developed in the 1990s by Dr Ann Cavoukian, former Privacy and Information Commissioner of Ontario, Canada.[25] The OAIC references Dr Cavoukian's work as the basis of its definition of privacy by design. The following is a summary of Dr Cavoukian's seven foundational principles developed by the UK Information Commissioner's Office.[26]

Proactive not reactive; preventative not remedial	You should take a proactive approach to data protection and anticipate privacy issues and risks before they happen, instead of waiting until after the fact. This doesn't just apply in the context of systems design – it involves developing a culture of 'privacy awareness' across your organisation.
Privacy as the default setting	You should design any system, service, product, and/or business practice to protect personal data automatically. With privacy built into the system, the individual does not have to take any steps to protect their data – their privacy remains intact without them having to do anything.
Privacy embedded into design	Embed data protection into the design of any systems, services, products and business practices. You should ensure data protection forms part of the core functions of any system or service – essentially, it becomes integral to these systems and services.
Full functionality – positive sum, not zero sum	Also referred to as 'win-win', this principle is essentially about avoiding trade-offs, such the belief that in any system or service it is only possible to have privacy or security, not privacy and security. Instead, you should look to incorporate all legitimate objectives whilst ensuring you comply with your obligations.
End-to-end security – full lifecycle protection	Put in place strong security measures from the beginning and extend this security throughout the 'data lifecycle' – ie process the data securely and then destroy it securely when you no longer need it.
Visibility and transparency – keep it open	Ensure that whatever business practice or technology you use operates according to its premises and objectives, and is independently verifiable. It is also about ensuring visibility and transparency to individuals, such as making sure they know what data you process and for what purpose(s) you process it.
Respect for user privacy – keep it user-centric	Keep the interest of individuals paramount in the design and implementation of any system or service, eg by offering strong privacy defaults, providing individuals with controls, and ensuring appropriate notice is given.

[24] Office of the Australian Information Commissioner (2018) *Guide to Securing Personal Information*, available from <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/#ftn21>
[25] Cavoukian, A (2011) *Privacy by Design: Seven Foundational Principles*, Information and Privacy Commissioner of Ontario, available from <https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>
[26] UK Information Commissioner's Office, *Data protection by design and default*, available from <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>

Appendix V
Lead data roles and responsibilities

The following pages provide a detailed overview of the data specific roles in each Directorate - the Executive Data Lead, the data custodian and the data steward.

The Executive Data Lead is accountable for things data in their directorate and will ensure that all datasets (both critical and non-critical) are assigned a Data Custodian and Data Steward.

Executive Data Lead		
Core role	• Accountable for overseeing and improving directorate data governance, management and use for internal and external data as an asset.	
Who is an Executive Data Lead?	• Senior executive level. • Lead internal and represent directorate on whole of government governance groups • Ideally, each directorate will appoint a designated Executive Data Lead or chief data officer to fill this role. An alternative is for these responsibilities to be an overt function of an existing role, such as Chief Information Officer, Director-General or Deputy Director-General.	
Responsibilities	• Establish and implement directorate data policies, data strategy, and roadmap. • Ensure a data custodian and data steward are assigned to all directorate datasets. • Champion data use and improve the maturity of the directorate's data practice. • Oversee a range of data functions that may include data capture, data sharing, data quality, data architecture, data science and analytics, business intelligence and data security. • Accountable for data architecture decisions and data standards for directorate data systems, in consultation with the broader whole of government network. • Facilitate the directorate's single sources of the truth, based on multi-source data. • Facilitate the establishment of information and data sharing agreements and arrangements. • Ensure and promote directorate datasets are registered in a data catalogue to enable discoverability by all staff and directorates. • Promote the release of high-value datasets on the ACT Government's Open Data platform.	
Data culture	• Champion and foster a data culture in the directorate; disrupt old ways of working. • Provide leadership and advice in safe and competent data practice. • Build digital and data literacy, and data practice maturity. • Work with Directorate executives to uncover data insights to inform strategies and practice. • Proactively encourage and remove barriers to information and data sharing. • Work across their network to resolve data duplication and conflicts. • Build public trust and improve public confidence in the safe, secure and trusted use of data, including by ensuring greater transparency and effective communication. • Ensure informed consent from the individuals for data capture and genuine alternatives for those who don't consent.	
Compliance	• Ensure data activities align with directorate and whole of government strategic vision. • Implement and comply with data strategies, policies and practices including the whole of government *Data Governance and Management Framework and Guide*. • Support measures to ensure processes to capture, manage and govern data comply with relevant legal and regulatory requirements.	
Safety and security	• Accountable for safe and competent data practice across the directorate. • Support data custodians and stewards to implement data protections and practices that uphold safe, secure and trusted use of data. • Be the first point of escalation for data sharing and compliance issues within and across directorates. • Establish a directorate data breach plan, in alignment with whole of government data protection principles, setting out how the directorate will contain, assess and respond to data breaches quickly, to help mitigate potential harm to individuals. • When there is a data breach, work with directorate data custodian, data steward and stakeholders to implement the response plan, and ACT Chief Digital Officer as appropriate.	
Supported by	• Data Custodians • Data Stewards • Business and System Owners • Privacy Officers • Records Officers and Freedom of Information Officers	• Government Solicitor's Office • Shared Services ICT • Territory Records Office • Office of the Chief Digital Officer
Skills/ knowledge/ capabilities/ training?	• Leadership, engagement and communication skills including story telling • High level understanding of working with data including design and delivery of high-value data analytics, data governance, data management and data infrastructure solutions • Skilled in developing and successfully implementing organisational strategies and plans	

Data Custodian		
Core role	• Accountable for governing and overseeing the management of one or more datasets assigned to them (including internal or external datasets).	
Who is a data custodian?	• Must be an identified position and role within the ACT Government. • Typically, senior executive level, although a data custodian's functions may be delegated to a subject matter expert within their branch. • Professional development plans should reflect the data custodian's understanding of the obligations associated with governing and managing their dataset/s.	
Responsibilities	• Supports the delivery of the directorate data policies, data strategy, and roadmap • Embeds the ACT data principles in data governance and management practice • Appoint and oversee a data steward for day-to-day management of the relevant dataset/s, including appropriate and accurate data documentation. • Authorise the capture, design or generation of data, that are consistent with data quality frameworks, common data model and master data. • Authorise safe and authorised sharing, access, use and release of data for public benefit. • Register datasets in a data catalogue to enable discoverability by all staff and directorates. • Identify and release high-value datasets on the ACT Government's Open Data platform at data.act.gov.au. • Escalate issues to Data Governance committees through directorate representatives.	
Data culture	• Support and strengthen a data culture in the directorate. • Provide leadership in good data governance and management practice. • Support and empower data users to make better-informed, data-driven decisions by making it easier to find and use existing data. • Encourage and support data sharing unless there is a legislative requirement not to share. • Fosters Directorate-wide understanding of good data governance and management practice in relation to new data captures or enhancement to existing datasets. • Strengthen relationships between stakeholders to support better use of government data. • Build public trust and improve public confidence in the safe, secure and trusted use of data, including by ensuring greater transparency and effective communication.	
Compliance	• Ensure data capture and sharing aligns with directorate and Government strategic goals. • Implement and comply with data strategies, policies and practices including the whole of government *Data Governance and Management Framework*. • Implement measures to ensure processes to capture, manage and govern data comply with relevant legislation and policy. • Understand legislative provisions that impact the safety, security and sharing of data.	
Safety and security	• Implement data governance practices that uphold safe, secure and trusted use of data. • Use the Five Safes Framework as a guide to govern data and make decisions about effective use and sharing of data • Ensure technical controls and safeguards are in place and data content and changes can be audited. • Establish a data breach plan for the directorate, and when there is a data breach, implement a quick and effective response and work with directorate's Executive Data Lead, Director-General or Deputy Director-General as necessary. • Understand how to identify sensitive or personal information in data that may be shared or released.	
Support	• Data Steward • Shared Services ICT • Territory Records Office • Office of the Chief Digital Officer	• Privacy officers • Records officers and Freedom of Information Officers
Skills/ knowledge/ capabilities/ training?	• Understanding of data governance and management functions, processes and tools • Understanding of data sharing, data protection, data security and risks • Understanding of data asset management and data licensing and procurement	

Data Steward		
Core role	• Responsible for the day-to-day operational management of one or more datasets assigned to them (including internal or external datasets). • Report to data custodian.	
Who is a data steward?	• Typically, Senior Officer Grade A level or equivalent, although a data custodian's functions may be delegated to the subject matter expert within their team. • Professional development plans should reflect the data steward's understanding of the obligations associated with managing their dataset/s.	
Responsibilities	• Supports the delivery of the directorate data policies, data strategy, and roadmap • Embeds the ACT data principles in data governance and management practice • Ensure all documentation relating to the dataset is clear and current, including dataset register/ catalogue, business glossary, master data, metadata and quality specifications. • Facilitate and maintain records of safe and secure sharing, access, use and release of data when authorised by the data custodian. • Register datasets in a data catalogue to enable discoverability by all staff and directorates. • Ensure data meets business requirements for all relevant line areas and is fit for purpose. • Support data users to use data appropriately, ie fit for purpose. • Identify and release high-value datasets on the ACT Government's Open Data platform at data.act.gov.au when authorised by the data custodian. • Escalate issues to Data Governance committees through directorate representatives. • Manage license arrangements for external datasets.	
Data culture	• Support and strengthen a data culture in the directorate. • Provide leadership in good data governance and management practice. • Support and empower data users to make better-informed, data-driven decisions by making it easier to find and use existing data. • Encourage and support data sharing unless there is a legislative requirement not to share. • Fosters Directorate-wide understanding of good data governance and management practice in relation to new data captures or enhancement to existing datasets. • Strengthen relationships between stakeholders to support better use of government data. • Build public trust and improve public confidence in the safe, secure and trusted use of data, including by ensuring greater transparency and effective communication.	
Compliance	• Ensure data capture and sharing aligns with directorate and Government strategic goals. • Work with the data custodian and support measures to ensure compliance with relevant legislation, policies, regulatory requirements, compliance standards and guidelines. • Support the implementation of data strategies, policies and practices including the whole of government *Data Governance and Management Framework*. • Report to data custodians and executives on compliance with directorate data strategy and whole of government *Data Governance and Management Framework* • Understand legislative provisions that impact the safety, security and sharing of data. • Communicate legislative and policy requirements to data users.	
Safety and security	• Implement data management practices that uphold safe, secure and trusted use of data, including ensuring data is protected from unauthorised access, change or use. • Use the Five Safes Framework as a guide to govern data and make decisions about effective use and sharing of data. • Provide information on potential risks and regulatory guidance to the data custodian. • When there is a data breach, inform the data custodian and work together to implement a quick and effective response. • Identify sensitive or personal information in data that may be shared or released.	
Support	• Shared Services ICT • Territory Records Office • Office of the Chief Digital Officer	• Privacy officers • Records officers and Freedom of Information Officers
Skills/ knowledge/ capabilities/ training?	• Understanding of data governance and management functions, processes and tools • Understanding of data sharing, data protection, data security and risks • Understanding of data asset management and data licensing and procurement	

Data Governance and Management Guide

August 2020

ACT Data Analytics Centre

Office of the Chief Digital Officer

ACT Government