NSW Data Governance Toolkit

Document number:	**Version number**: 1.0
Date: Thursday, September 17, 2020	

Contact details

Name: Data Analytics Centre, Data.NSW Department of Customer Service
Email: datachampions@customerservice.nsw.gov.au

September 2020

Table of Contents

1. Introduction

1.1 Introduction to the Toolkit

When used effectively, data can provide governments with rich insights about their customers and communities, aid in decision-making, and ultimately drive better outcomes that people can really see and feel. To ensure government decision-making is truly evidence-based and customer-driven, agencies need timely access to trusted, accurate and reliable data. It is therefore critical that government data assets are governed effectively.

Good data governance is important because it is the mechanism by which agencies can oversee, monitor and control the management of their data. It is critical to the NSW Government's ability to extract value from data assets, share data across the public and private sector in a safe and secure way, and use this data to address shared policy challenges and attain whole-of-government policy objectives.

While there are exemplars of good data governance practice across the NSW Government, many agencies operate in an ad hoc way, leading to inconsistency in how data is collected, managed, used and shared across government. To achieve the potential gains from the exponential volumes of data being created, and to ensure a coordinated approach to achieving policy objectives, agencies need a consistent approach to data governance that is built on a common understanding of its benefits, obligations and best practice.

1.2 Purpose of the Toolkit

This Toolkit has been developed to provide NSW Government agencies with practical and consistent guidance on the key components of an effective data governance program, as well as to create a shared understanding of what good data governance looks like.

While compliance with this Toolkit is not mandatory, following the guidance in the Toolkit will:

- support agencies to maximise the value of data while reducing data-related risk;
- assist agencies in meeting their legislative and regulatory obligations;
- ensure data is managed in line with national and international standards;
- facilitate better interoperability between agencies; and

- build data governance maturity at both the departmental and all-of-government levels.

This Toolkit does not prescribe a one-size-fits-all approach to data governance. Each agency should consider its needs, organisational environment, and capacity to implement the guidance and adapt it in ways that make most sense for their organisation.

1.3 Scope of the Toolkit

The Toolkit provides guidance on:

- the principles that underpin effective data governance;
- the legal and regulatory environment in which agencies operate;
- how to set up data governance structures, roles and responsibilities;
- the organisational enablers required to drive data governance maturity; and
- the data management functions that support data governance.

Which data assets does the Toolkit apply to?

The Toolkit applies to all data of business value which is collected, created, used and stored by NSW Government agencies. This includes both new and legacy data assets.

1.4 Audience of the Toolkit

The primary audience of the Toolkit is NSW Government agencies who have identified a need to better plan, monitor and control their data. The Toolkit is primarily intended for organisational data governance bodies, senior executives, business users, data custodians, and any staff who are interested in learning more about data governance.

Local government, State Owned Corporations (SOCs), and entities funded by the NSW Government may also find the Toolkit useful. However, it is important to note that some of the legislative or policy obligations outlined in the Toolkit may not apply to organisations outside of the NSW Government.

1.5 Structure of the Toolkit

The Toolkit contains twelve modules that are designed to help agencies improve their ability to govern their data. The modules are:

1) Introduction to data governance
2) Legal and Policy Context
3) Data Governance Model

4) Strategy and Planning

5) Organisational Structures

6) Assigning roles and responsibilities

7) Leadership

8) Data-driven culture

9) Workforce skills and capability

10) Technology

11) Data Management

12) Data Governance Checklist

Depending on the agency's needs, the Toolkit can be read in its entirety or users can select the module relevant to their data governance needs.

1.6 How was the Toolkit developed?

This Toolkit has been developed through a consultative process with data users and subject matter experts across the NSW Government. The NSW Government's Data Champions Network has played a key role in its design and the Toolkit will benefit from ongoing input from Network members, as well as local, state and federal public sector agencies.

1.7 Maintaining the Toolkit

To ensure the Toolkit continues to meet agency needs, the Toolkit will be regularly reviewed and updated as data needs change, data governance and management technologies evolve, standards develop, and best practice matures.

Agencies and other users of the Toolkit are encouraged to contribute to and provide feedback on the Toolkit by emailing: DataChampions@customerservice.nsw.gov.au

2. Introduction to data governance

2.1 What is data governance?

The Data Management Body of Knowledge defines data governance as “the exercise of authority, control and shared decision-making (planning, monitoring and enforcement) over the management of data assets” (DMBOK, 2017). Put simply, data governance is about implementing a set of policies, processes, structures, roles and responsibilities to ensure that an agency’s data is managed effectively, and that it can meet both its current and future business requirements.

> *Source:* DAMA Guide to the Data Management Body of Knowledge, Edited by M. Brackett, S. Early and M. Mosley. Bradley Beach, NJ: Technics Publications LLS, 2017 (second edition).

2.2 Why is data governance important?

Data governance is as important to an agency as any other corporate, business or IT governance process. It ensures that data is understood, trusted and appropriately used. It ensures that the people who collect, manage and use data understand their responsibilities and see the value it adds to their work, the objectives of the organisation, as well as broader agency outcomes. Data governance is also an exercise in risk management because it allows agencies to minimise risks around the data it holds, while extracting the maximum value from it.

2.3 What are the benefits of data governance?

Data governance, like any other program or process, must have a clear purpose for it to be beneficial. Instead of doing data governance for its own sake, it should be established to help an agency achieve its strategic objectives and it should be closely aligned to their business needs.

When data governance is aligned to the organisation’s needs, it can deliver specific benefits across three areas: business value, efficiency and risk mitigation.

Business value

- Improved decision-making by ensuring decisions are based on higher quality data
- Increased competitiveness through improved customer satisfaction

- Increased public trust through improved data management and transparency

Efficiency

- Reduction in duplication and waste created by information silos
- Increased data sharing through improved trust and standardisation
- Reduction in costs by improving resource and process efficiencies
- Reduction in time spent by employees finding, acquiring and processing data

Risk mitigation

- Reduction of risk and costs as data is better managed to support regulatory compliance
- More robust consideration of ethical and privacy issues to avoid reputational damage

Source: Adapted from Information Governance ANZ

2.4 Guiding principles of data governance

The NSW Information Management Framework principles should guide agencies in governing and managing their data:

1) **Data is business enabling, aligned to business needs and customer outcomes**

   Data is created and managed so that it directly supports organisational, business and customer requirements. Data is integral to government's operations and effectiveness.

2) **Data is secure, valued and managed as an asset**

   Data is recognised as a core component of government services and operations, and is supported and maintained as a secure, long-term business asset wherever required.

3) **Data is trustworthy, used and reused with confidence**

   Data is accurate, authentic and trusted, allowing its ongoing use and reuse by government and the community.

4) **Data is high quality and (where relevant) spatially enabled**

Quality data is of value to customer, business and strategic objectives, and where relevant, spatial enablement allows for improved service planning, delivery and business insights.

5) **Data is managed across the full lifecycle, protected from unauthorised use and inappropriate deletion**

   Data is appropriately managed from procurement or service design, through to creation and to final disposition. This management includes the protection of personal, health and sensitive information, and prevention of deletion until enabled by legal destruction and authorisation.

6) **Data is available and open to the community and government**

   Where appropriate, data is publicly accessible and available in accordance with proactive release and open data principles, or shared within and between organisations to improve policies, services, planning and innovation.

3. Legal and Policy Context

The Toolkit has been designed to support NSW Government agency compliance with relevant all-of-government statutes, policies and frameworks that relate to the collection of data, data management and retention, confidentiality, data sharing, data linkage and public release.

3.1 Legislative requirements

Legislative instruments relating to the Toolkit include:

- ***Government Information (Public Access) Act 2009*** **(NSW)**

The GIPA Act facilitates public access to NSW Government information. It does this by authorising and encouraging the release of information by NSW Government agencies, giving members of the public the right to request access to government information, and by ensuring government information is only restricted where there is an overriding public interest against disclosing the information.

- ***Privacy and Personal Information Protection Act 1998*** **(NSW)**

The PPIP Act provides for the protection of personal information, and the protection of the privacy of individuals generally. Under the Act, all personal information that is made, kept or collected by government organisations must be created and managed in accordance with the Information Protection Principles under the PPIP Act. The Information and Privacy Commission website has an overview of NSW privacy legislation.

- ***Health Records and Information Privacy Act 2002*** **(NSW)**

The HRIP Act protects health records and information by protecting the privacy of an individual's health information held by the public and private sectors, enables individuals to gain access to their information and provides an accessible framework for the resolution of complaints regarding the handling of health information. The 15 Health Privacy Principles are legal obligations that agencies must abide by when collecting, holding, using and disclosing a person's health information.

- ***State Records Act 1998*** **(NSW)**

The State Records Act sets out the rules for the creation, capture, control, use, maintenance and disposal of all records and information in line with whole-of-government records and information management policies. The NSW State Archives & Records Authority has developed the Records and Information Management Policy checklist that

helps agencies ensure their internal strategies are consistent with whole-of government information management policy.

- ***Data Sharing (Government Sector) Act 2015* (NSW)**

The Data Sharing Act enables the sharing of data between NSW Government agencies, and with the Data Analytics Centre (DAC). The Act encourages and facilitates data sharing, outlines safeguards for sharing data, states that data sharing must be legally compliant, ensures data involving personal information is protected, and allows the responsible Minister to direct agencies to provide data to the DAC under certain circumstances.

3.2 Policies and other guidance

Policies and other guidance relating to the Toolkit include:

- ***NSW Open Data Policy***

Data should be open to the extent that its management, release and characteristics meet the objectives of openness, accountability, fairness and effectiveness set out in the *Government Information (Public Access) Act 2009* (NSW). Under the GIPA Act, there is a presumption in favour of the disclosure of information, unless there is an overriding public interest against disclosure.

The Policy sets out six open data principles that all government data must be:

1. Open by default, protected where required;
2. Prioritised, discoverable and usable;
3. Primary and timely;
4. Well managed, trusted and authoritative;
5. Free of charge where appropriate; and
6. Subject to public input.

- ***NSW Cyber Security Policy***

The Policy sets out mandatory requirements that all agencies must comply with to ensure that cyber security risks to data, information, and systems are managed and data is kept secure. These include: implementing cyber security and governance; building and supporting a cyber security culture across the agency; managing cyber security risks and reporting against the Cyber Security Policy Requirements.

- ***NSW Data and Information Custodianship Policy***

The Policy defines a set of principles for the management and maintenance of the State's core data and information assets as well as outlining custodianship roles and responsibilities. Implementation of this policy and adherence to its principles facilitate compliance with the NSW Information Management Framework.

- ***NSW Information Management Framework***

The Framework sets out the core characteristics of 'information' for the NSW Government, which includes data and records, as well as a shared whole-of-government direction for information management. It sets out the vision, principles, minimum requirements, governance and capabilities for effective information management across the public sector. The Data Governance Toolkit expands on the data governance-related components of the Framework.

- ***NSW Information Classification, Labelling and Handling Guidelines***

The Guidelines set out the NSW Government's approach to classifying, labelling and handling sensitive information. The classification of information created, owned and managed by the NSW Government is a mandatory requirement under the NSW Cyber Security Policy. The Guidelines are consistent with the Australian Government security classification system.

Additional legal, regulatory and policy requirements may apply in specific agency or business domains. All organisations should identify the specific requirements that apply to their environment.

3.3 State, National and International standards

State, National and International standards already exist with respect to data governance. All NSW public sector agencies are responsible for conforming to appropriate standards, including those issued by State Records NSW and the Information and Privacy Commission NSW.

Standards specific to data management are included in the Data Management component of this Toolkit and are based on the internationally recognised Data Management Body of Knowledge guide.

> *Source*: DAMA Guide to the Data Management Body of Knowledge, Edited by M. Brackett, S. Early and M. Mosley. Bradley Beach, NJ: Technics Publications LLS, 2017 (second edition).

While this Toolkit will be updated to reflect ongoing developments in standards and best practice, public sector agencies are expected to maintain their understanding of current applicable standards.

4. Data Governance Model

Outlined below is a practical model that has been designed to assist NSW Government agencies to develop or strengthen data governance maturity in their organisation. The Data Governance Model (*'the Model'*) brings together all the components that are vital for any data governance program, regardless of the agency.

4.1 What does the Model cover?

The Model defines four interconnected tiers of data governance activities, each of which is critical to effective data governance in agencies. The four tiers are:

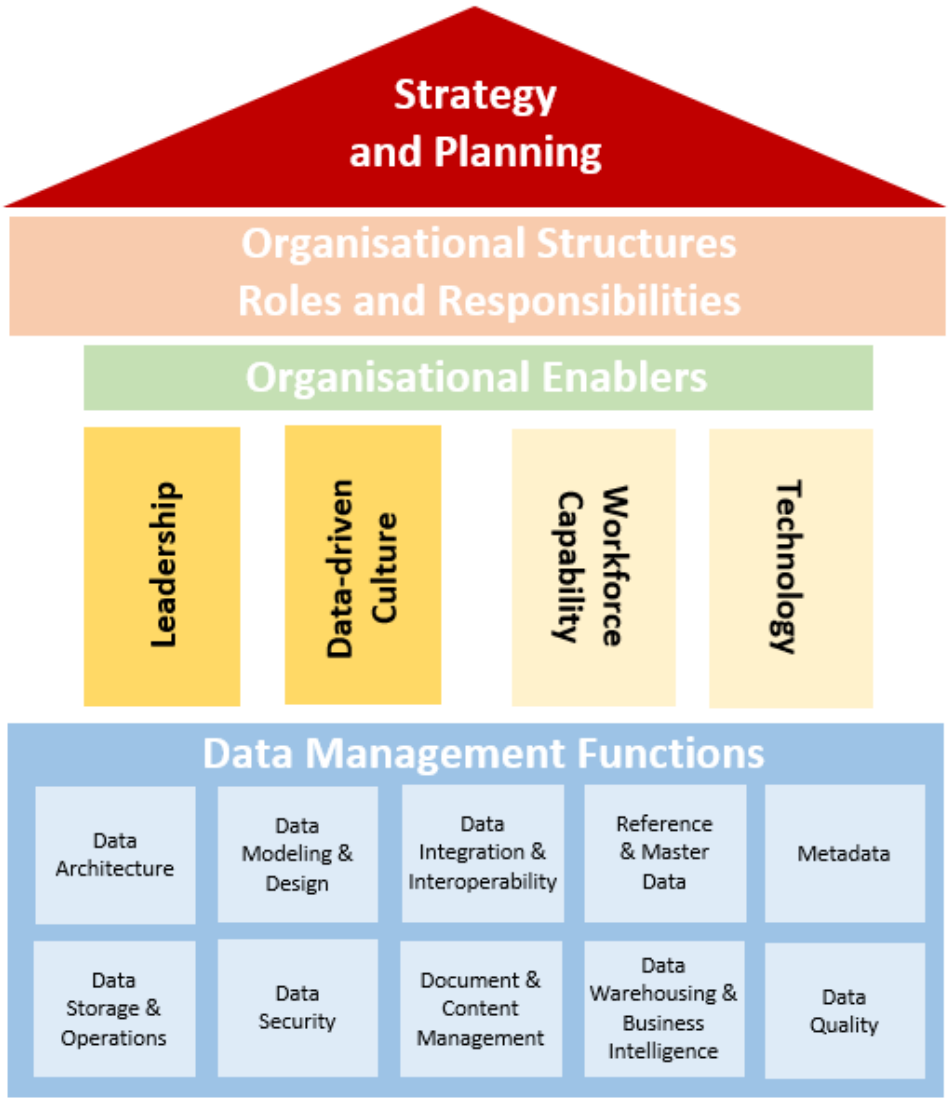
1) **Strategy and planning** – agencies clearly define the data governance program's values, vision and mission and compose a business-aligned strategy for governing and managing data as an organisational asset.

2) **Organisational Structures** & **Roles & Responsibilities** – agencies ensure accountability and decision-making authority for data-related activities are appropriately assigned and formalised at all levels of the organisation.

3) **Organisational Enablers** – agencies ensure the organisational environment is an enabler of good data governance. This means ensuring there is a strong *motivation* (or 'will') to achieve good data governance by having sustained buy-in and investment from senior leadership, as well as fostering a strong organisational data culture. It also means ensuring the organisation has the requisite *capability* (or 'skill') to achieve good data governance, both in terms of workforce capabilities, as well as appropriate tools and technologies.

4) **Data Management** – agencies ensure their data governance program has oversight of core data management functions (e.g. data quality, storage, security, business insights etc.).

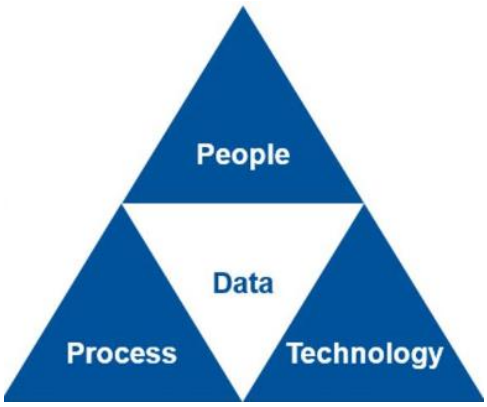
Figure 1: Data Governance Model



4.2 Interpreting the Model

Each component of the Model, outlined in detail in the following modules, includes a high-level summary of ***what*** the component is, ***why*** it is important, what good practice looks like (i.e. the ***goals***), ***how*** to achieve good practice and, where appropriate, provides references to useful resources and relevant standards. The level of detail for each component has been kept to a high level and we intend to expand the practical elements of the framework gradually with input from agencies.

The Model also aligns with Gartner's (2017) 'Golden Triangle' of '**People**, **Process** and **Technology'** (with **Data** at the centre), which recognises that effective data governance is an ongoing effort executed by people, enabled by repeatable processes, and supported by technology. Each component of the Model therefore encompasses a mix of accountabilities relating to people, processes and technologies to support the implementation of that component.



Source: Gartner 2017

5. Strategy and Planning

5.1 What is it?

A fundamental premise of data governance is that data is governed to meet the needs of the business. An agency's data governance program should be driven by the strategic priorities of the organisation. For example, if poor data quality is preventing an agency from achieving a key strategic outcome, then the focus of the data governance program would be on improving data quality. If having a single view of the customer (SVOC) is important, then Masterdata management would be prioritised in the data governance program. Of course, agencies may need to focus on more than one issue at once. While it is likely that agencies will have a range of strategic objectives, these should be prioritised and addressed incrementally by the data governance program over time.

5.2 Why is it important?

Having a clear business-aligned strategy for your agency's data governance program will ensure that data governance and management activities support the achievement of desired business outcomes. It will also ensure that the data governance program delivers tangible benefits to the organisation in the short-term. By demonstrating the value of data governance for the organisation, this should allow you to gradually build staff and senior executive buy-in for your data governance initiatives and allow you to scale the program across the organisation. A targeted and incremental approach that positively impacts the organisation is far more likely to succeed in the long-term.

5.3 What good looks like

- **Business-aligned**: the data governance program is tailored to the agency's business needs and strategic objectives.
- **Compatible**: the data governance program takes into consideration specific organisational constraints and is compatible with the cultural context.
- **Incremental**: the data governance program is implemented incrementally across the organisation and initiatives are prioritised based on risk and value.
- **Measured**: data governance and management initiatives are monitored, analysed and measured to ensure that interventions are achieving desired outcomes.

- **Collaborative**: the data governance program is agreed by key stakeholders across different functions of the organisation and all staff participate in implementing good data governance practices.
- **Communicated**: the vision for the data governance program and its alignment with the agency's strategic objectives should be communicated to staff at all levels.

5.4 How to achieve good practice

- **Define the core business problem(s) you are trying to solve**. Below are some questions that will help you to do this:
    1. What problem are you trying to solve?
    2. What outcomes do you want to achieve?
    3. How will data work to meet your agency's needs?
    4. What kinds of data does your agency need access to?
    5. How are you going to track, assess and monitor progress?
- **Analyse the current state by undertaking a data maturity assessment**. Once a business problem has been identified, it is useful to undertake a data maturity assessment in order to understand the context in which the problem is occurring and identify focus areas for your data governance program.
- **Identify focus areas for your data governance program.** This should be done by working with stakeholders across all functions of the organisation to determine what data governance activities will have the greatest impact on the business. An agency may have a multitude of focus areas, so it is important to start small and prioritise based on business value.
- **Plan your governance response**. Once the focus areas have been selected, decide what data governance mechanisms – such as policies, procedures, processes, standards, structures – will be implemented to ensure the resolution of the problem.
- **Develop metrics to assess whether the data governance response is helping to solve the problem.** Start small and set SMART goals (specific, measurable, attainable, result-oriented, time-bound) with clear metrics to assess whether the response is achieving desired outcomes.
- **Communicate the success of data governance interventions to staff** to ensure that they understand how the data governance program aligns with the agency's strategic objectives.

- **Repeat the process.** As with all large and complex projects, the key to success is to start small, address a well-defined problem, communicate the outcomes of the intervention to staff, and repeat the process and allow the program to scale gradually.

! *As organisational and data needs change and data volume and complexity increase, decisions about how to govern data will need to evolve. A formalised enterprise-wide strategy and process for making these policies and decisions will need to be in place and be continuously monitored and updated to drive business improvements.*

6. Organisational Structures

6.1 What is it?

One of the most important aspects of data governance is ensuring the right organisational structures are in place to ensure data-related priorities and initiatives are aligned across the agency. This alignment happens via organisational bodies, often referred to as data governance boards, councils, steering committees or working groups. These bodies are generally comprised of stakeholders from across different business functions who have the authority to make strategic and operational decisions. While these groups often have different functions and roles, an important component of this structure is having an overarching decision-making body that assumes accountability for the strategic direction of data governance in the agency.

6.2 Why is it important?

Without the right organisational structures in place, data flows in and out of different parts of the organisation, with nobody empowered to take responsibility for its entire journey through various systems, databases and processes. This leads to inefficient and contradictory data management practices, and results in poor quality and under-utilised data. A data governance structure, with clearly assigned decision-making authority, provides your agency with a mechanism to develop a consistent, systematic and efficient approach to maximising the value of data.

6.3 What good looks like

- **Cross-enterprise:** the organisational structure includes stakeholders from across the various business areas of the organisation to support enterprise-wide decision-making.
- **Executive-representation**: the organisational structure includes a senior executive body that has the capacity to implement enterprise-wide data governance initiatives.
- **Targeted:** working groups are engaged to address discreet data issues, such as data quality improvement, privacy and security.
- **Contingent**: the organisational structure is tailored to the agency's specific needs, strategic priorities, size, resources and its current level of data maturity.

6.4 How to achieve good practice

- **Ensure there is a cross-functional executive-level body that has strategic oversight of data governance decisions and activities across the organisation**. Although developed for information governance, refer to the National Archives of Australia sample terms of reference for an information governance committee for direction on how to set up a data governance body.
- **Ensure the data governance structure is compatible with your agency**. There is no “right” way to organise a data governance structure. While some agencies establish formal data governance bodies, others may choose to integrate data governance responsibilities into existing governance groups. The important thing is that data governance decisions are made collaboratively among staff and across business areas.
- **Establish working groups for driving discreet data projects**. These bodies can also provide feedback to the executive-level governance body regarding the effectiveness of data governance initiatives within the business areas.
- **Develop a visual representation of your organisational data governance structures** that is accessible to all staff.

! *Although setting up an organisational data governance structure may only take a few months, incorporating its recommendations into business-as-usual may take significantly longer. Agencies should commit to regular data maturity assessments to guide the work of the data governance body and ensure it is focusing on priority areas of improvement.*

7. Assigning roles and responsibilities

7.1 What is it?

While good data governance is everyone's responsibility, agencies need to clearly define the key people who will be responsible for governing and managing data across the organisation. Assigning responsibilities to specific roles ensures there are specific people within the organisation who are responsible for ensuring that data is appropriately managed throughout its lifecycle.

The NSW Data & Information Custodianship Policy directs the development and implementation of data and information custodianship roles and responsibilities. It also includes a Custodianship Model that sets out specific data and information roles. While the use of a standardised model can be a key enabler of cross-agency collaboration, in practice it is recognised that many variants of this model exist across the NSW Government. This is because how agencies assign roles across an organisation tends to depend on many factors – most importantly, the data maturity and size of the agency.

To ensure this Toolkit meets agency needs, outlined below is an adapted version of the Custodianship Model. The adapted model is specific to data (i.e. excludes information management) and describes the roles in functional terms rather than using traditional role titles (e.g. Data Custodian, Data Steward, Data Owner, Data Sponsor). The purpose of this is to ensure that people are assigned responsibility for undertaking these functions, and to allow agencies to assign these functions in ways that work for them.

Function	Main Responsibilities
Accountable Executive Accountable Executives have **accountability** for the data and are generally the responsibility of the Agency Head (Secretary, Chief Executive, or equivalent authority), however this role is often delegated to a designated Senior Executive. This role is typically referred to as the Data Sponsor or the Data Owner.	• Approve policies, protocols and guidelines in relation to the data asset, process and/or system • Ensure that all legal, regulatory and policy requirements are met in relation to the data assets management • Approve significant changes to the data collection, process and/or system • Approve budget and resourcing/provide funding for data management projects • Monitor the performance of data governance responsibilities and identify improvements • Ensure data assets held by the agency are identified and documented in a data catalogue or register of data assets • Delegate responsibilities for decisions and tasks to Responsible Executives.

Responsible Executive Responsible Executives are generally Directors with delegation from the Accountable Executive to exercise overall **responsibility** for a specified data asset. This role is typically referred to as the Data Custodian.	• Enforce the rules on behalf of the Accountable Executive • Identify and document data assets held in a data catalogue or register of data assets • Identify the information security classification of data assets to ensure appropriate protection and handling of the information • Determine the conditions for appropriate collection, storage, use and sharing of the data and approve data change requests, data sharing requests and open data release • Agree and set the standards for the data asset • Nominate the Operational Data Manager for data assets and ensure responsibilities are fulfilled • Develop a strategic plan for the use and management of the data asset.
Operational Data Manager Data Managers are generally business managers, process owners or subject matter experts with the greatest operational stake in the content of the data asset. They are responsible for operational (**frontline**) data management and for stewarding the data through the data pipeline. This role is sometimes referred to as the Data Steward and is seen as the 'gatekeeper' to accessing the data asset.	• Day-to-day operational management and operation of the data asset • Ensure data is shared under an agreement or license to ensure privacy, security and data quality are maintained • Manage the data asset in compliance with relevant legislation, policies, standards and any conditions specified by the Responsible Executive • Work with stakeholders to develop and maintain metadata including a data dictionary, business rules and guide for use • Provide advice to the Responsible Executive on the management of the asset • Provide advice on the proper use and interpretation of the data to Data Users • Provide feedback to Data Creators in relation to data quality issues and the resolution of errors in the data.
Data Creator Data Creators are any employee, contractor or consultant who captures or creates data on behalf of the agency, to be processed as a data asset. This role is sometimes referred to as the 'Supplier' of data to government.	• Ensure data is recorded or collected according to agreed data standards and liaise with the Accountable or Responsible Executive on standard requirements • Ensure data is accompanied by accurate and sufficiently detailed metadata that enables people to understand it (e.g. creating a data dictionary, recording your methodology and how the data was created) • Ensure processes are in place for the ongoing maintenance of the data • Ensure data security • Comply with legislation, policies and terms and conditions associated with data collection, including consent where applicable.

Data User Data Users can be anyone, public and government, who uses government data.	• Acknowledge the source of data and abide by any copyright or licensing requirements when using data • Understand the data and ensure it is fit for its intended purpose • Report any errors or omissions to the Operational Data Manager or Responsible Executive regarding data they receive in a timely manner • Comply with terms and conditions of the license or agreement for access to data. • Comply with legislation, policies and standards • Ensure security and privacy are maintained whenever data is accessed • Report any breach or suspected breaches to the Operational Data Manager and/or Responsible Executive in the first instance • Obtain approval from the Accountable Executive or delegated authority for release of data.

7.2 Why is it important?

Under the *State Records Act 1998 Act* (NSW), agencies are responsible for the creation, management, protection and maintenance of their data, even when these management responsibilities have been delegated to another agency. It is important that agencies assign staff specific data responsibilities to ensure data is managed appropriately across its full lifecycle. A clear understanding and acceptance of custodianship roles and responsibilities can also help maximise benefits and minimise costs associated with data management for agencies, and lead to greater efficiency along data value chains.

7.3 What good looks like

- **Assigned**: responsibilities are defined and formalised across the organisation and at all stages of the data lifecycle.
- **Appropriate**: responsibilities are appropriately matched with the responsible person's skills, expertise and delegation level.
- **Understood**: while some staff are formally assigned data management roles, all staff who handle data understand the data responsibilities associated with their role.
- **Shared**: data responsibilities are spread across all levels of the organisation and are not just the responsibility of the IT department, a specific data governance body or team.

- **Specified**: data sharing agreements and service arrangements clearly specify data rights, including whether responsibilities for the data will be transferred to a third party.

7.4 How to achieve good practice

- **Assign data responsibilities across the organisation** and ensure the data is mapped to the responsible person(s) in a data catalogue.
- **Develop a data governance framework or policy that specifies who is responsible for the various aspects of the data**, including who is responsible for giving permissions for open release and data sharing.
- **Formalise data responsibilities where they already exist** and avoid assigning responsibility to anyone who is not already undertaking the role in their day-to-day work.
- **Ensure responsibilities are matched to the responsible person's skills, expertise and delegation level**. If parts of your agency lack data expertise, recruit new staff or leverage staff in different areas of the agency with specialised data skills.
- **Ensure staff with specific data responsibilities are provided with training and supported by workflow tools** that make their jobs easier.
- **Ensure data sharing agreements specify data rights,** including whether ownership of the data will be transferred to a third party.
- **Develop a visual representation of your organisation's data roles and responsibilities** that is accessible to staff within the organisation, as well as other agencies.

8. Leadership

8.1 What is it?

Strong and sustained leadership, advocacy and funding from senior executive leaders are important success factors for any data governance program. The leadership is responsible for setting direction, motivating employees, investing in and developing the necessary people skills required to manage and extract value from the data. Senior leadership should provide the high-level support needed to drive the data agenda of the agency and play a key role in facilitating collaboration across business functions to ensure data-related decisions are aligned with the agency's strategic objectives.

8.2 Why is it important?

Without strong leadership support and engaged executive sponsors, obtaining the funding, resources and alignment necessary for data governance may be challenging. Leaders are in a unique position to communicate the degree to which the agency values data as a strategic asset. Embedding data governance also generally requires some level of transformation within the organisation. Engaging the buy-in of individuals that are sufficiently senior and that can champion the data governance program across the organisation will help facilitate change management.

8.3 What good looks like

- **Sponsorship:** Senior leadership display strong, explicit and ongoing commitment for data governance
- **Investment**: Senior leadership recognise and address data resource needs and infrastructure requirements to support data governance
- **Participation**: Senior leadership participate in decision-making on important opportunities and risk mitigation issues relating to organisational data assets
- **Collaboration**: Senior leadership collaborate across different areas of the organisation to break down information silos, including risk and compliance, cyber security, data analytics and privacy

8.4 How to achieve good practice

- **Develop and deliver training in data for executives**, enabling them to make informed decisions and have a data and evidence-first mindset
- **Set up a data governance decision-making body** that comprises cross-functional leaders from across the organisation
- **Incorporate data metrics and goals into corporate plans and public reporting** and monitor and regularly report on progress
- **Build data use and analytics into organisational strategies and plans**
- **Appoint a member of the senior executive to lead and champion the organisation's data governance agenda**

9. Data-driven Culture

9.1 What is it?

Creating an organisational culture that values data as an asset is a core component of any data governance effort. However, changing entrenched organisational behaviours is widely regarded as the biggest obstacle that can derail data governance efforts before they even begin. Creating a data-driven culture means shifting the mindset of employees so that they are motivated to manage and use data effectively on a day-to-day basis. It involves raising awareness, knowledge and acceptance of an agency's data objectives, embracing innovation and change, and encouraging an open and transparent data culture.

9.2 Why is it important?

When data is not regarded as a strategic asset by staff across the organisation, data quality degrades, information silos proliferate, and inefficiency and poor decisions often follow. In many respects, a data-driven culture will follow naturally if there is strong commitment from senior leadership, staff have a basic level of data literacy, and specialised data capabilities are spread evenly across the organisation. However, creating this culture also requires an ongoing effort by senior leadership to ensure data is fully appreciated by staff across all areas and all levels of the organisation.

9.3 What good looks like

- **Enterprise-wide:** data governance is regarded as an enterprise-wide objective that applies to all staff, rather than just a compliance task or something for IT to do.
- **Celebrated:** staff that demonstrate good data management practices are celebrated by senior leadership.
- **Collaborative:** all parts of the organisation are engaged on enterprise-wide data governance initiatives and input from staff is incorporated from day one.
- **Business-enabler:** staff have a strong understanding of how data governance can help them do their jobs more effectively and deliver real value for customers.
- **Ethical:** robust data management practices are considered by staff as an ethical imperative, rather than a compliance requirement.

9.4 How to achieve good practice

- **Develop a simple and targeted communications plan** that aligns data governance initiatives with the agency's overall mission and objectives.
- **Develop and deliver learning opportunities and resources** that grow the data literacy of the entire organisation and give staff practical guidance on how they should manage data on a day-to-day basis.
- **Measure the effectiveness of data initiatives and share the results with staff as well as other agencies to promote a government-wide culture of learning about data governance**. For example, hold a showcase or create a data story to share the results of the data program or project and communicate how it contributes to the agency's mission and goals.
- **Ensure each business unit has an assigned data leader** to champion and engage with staff on data governance decisions and initiatives.
- **Develop performance metrics and incentivise and reward staff** that demonstrate and promote data-driven values and behaviours.
- **Set up a Community of Practice (CoP) for staff across the organisation who can lead and advocate for the agency's data agenda**. The CoP should have executive sponsorship and comprise relevant subject matter experts (SMEs) across the organisation, including security, information and record management, and privacy.

10. Workforce skills and capability

10.1 What is it?

Data skills and capability are core elements of effective data governance. All agencies need to be supported by a workforce that has the right set of skills and capability to manage and use data effectively. This means ensuring all staff have a basic level of data literacy and that there are enough staff with specialised data skills spread across the organisation. Specialised data skills include the ability to manage and analyse large amounts of data, implementation and management of data systems, data engineering and cyber security.

10.2 Why is it important?

Data skills and knowledge are essential for all NSW Government employees to support evidence-based decision-making, whether in policy development, program management or service delivery. These skills also assist in improving operational efficiency, raising service delivery standards, and improving stakeholder engagement. Inadequate data literacy can not only impact the ability of the agency to extract value from the data they collect, it can also leave agencies vulnerable to privacy and security breaches.

10.3 What good looks like

- **Data-literate**: all staff have a foundational level of data literacy.
- **Specialised**: staff with specialised data skills are spread evenly across the organisation and can be leveraged when required.
- **Development-focused:** senior leadership support the professional development of data skills and awareness across all levels of the organisation.
- **Cross-disciplinary**: teams have the right combination of technical data skills, as well as non-technical policy, project and business acumen.
- **Training**: staff have access to data skills resources and are trained in relevant governance policies and procedures.

10.4 How to achieve good practice

- **Assess workforce skills and capabilities needs**. A capability assessment will help facilitate a conversation within the organisation to identify and address data skills and capability gaps.
- **Develop a workforce strategy to address data skills and capability gaps**. The strategy should include the development of training, resources, and education to build and develop individual capabilities. It is best practice to include a mix of face-to-face, discussion-based and leadership-led training as well as self-guided online training. For self-guided learning resources, refer to the NSW Data Skills – Learning Resources and the APS Data Literacy Learning Guide.
- **Invest in the development and recruitment of staff with specialised data skills**. The following examples provide a good reference point for identifying the skills required across teams, as well as the agency as a whole:
    - Data analyst – manipulate and interpret data for decision making and to solve problems
    - Data policy and law expert – monitor the effectiveness of controls, resolve compliance challenges, advise on legal rules and controls to meet applicable legislation and standards
    - Data scientists – are hybrid experts in analysis and software programming, possess strong business acumen, coupled with ability to communicate findings
    - Data infrastructure engineers – support the infrastructure required to make data applications and platforms available in agencies and across the public service
    - Data architects – ensure the design of data systems, provide technical support for systems to undertake analysis.
- **Establish multidisciplinary teams to achieve skill-sharing and optimal project outcomes**. If there is a lack of data expertise in your agency, engage staff with specialised data skills during the stage when the skill is required.
- **Ensure role descriptions include the skills and capabilities** relevant to the data governance and management activities staff are expected to undertake.

11. Technology

11.1 What is it?

With the increasing speed, volume and complexity of data, it is becoming more and more challenging for humans to manage and use data in a cost-efficient and timely way. Although technology is not a solution on its own, it can be a significant enabler of data governance by simplifying and automating data management practices. When used appropriately, the right tools can assist with data monitoring and management, data security and privacy protection, and data lineage tracking. Tools can also be used to improve the quality of the data with automated validation, data cleansing and data enrichment.

11.2 Why is it important?

Data governance systems that rely heavily on humans to manually manage and monitor data, face much higher risks than systems that automate data management practices. Despite good intentions, human error almost inevitably creeps into data processes. These errors can lead to false and duplicated information, and ultimately undermine the agency's data governance efforts. While automating data governance won't remove the risks of this entirely, it can help agencies discover, manage and monitor these risks more easily. Technology solutions can also increase operational efficiency by freeing staff from manual, time-consuming and inefficient processes.

11.3 What good looks like

- **Automated**: data governance policies and processes and data management workflows are automated, where appropriate.
- **Enterprise-wide:** technologies break down organisational data silos and are implemented enterprise-wide, where appropriate.
- **Interoperable:** technologies support standard formats allowing interoperability across the organisation.
- **Secure:** technologies are compliant with security standards and ensure the privacy and protection of data holdings and use.

- **Future-proofed:** agencies consider their potential future needs as well as changes in regulations, technologies and other factors when selecting tools.

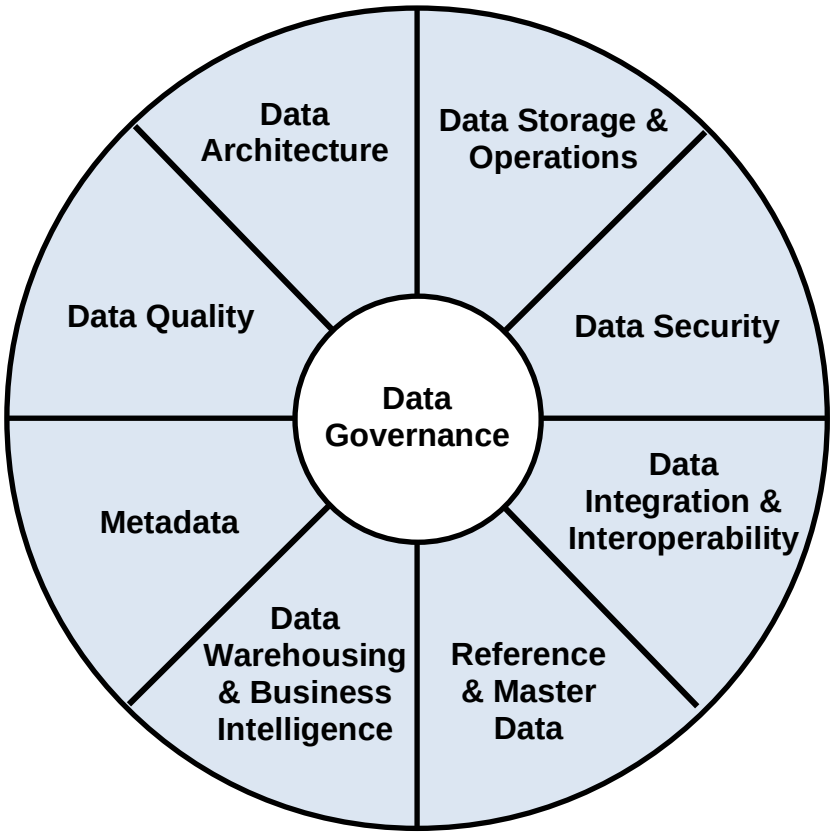
11.4 How to achieve good practice

- **Adhere to the "people and process before technology" approach** by ensuring that data governance processes are well-defined before they are automated with technologies.
- **Assess the current state technical capabilities and architecture of the organisation** and identify and prioritise focus areas for improvement and automation.
- **When selecting technologies to support data governance efforts, agencies should consider**:
    - Is it open source, scalable, and easy to integrate with the organisation's existing business processes?
    - Does it meet government standards regarding data sovereignty, privacy, and cyber security?
    - Can it provide effective data quality management (i.e. rules, profiling, reporting)?
    - Does it provide metadata support for document information security classification and data lifecycle management?
    - Does it assign and manage data governance roles and responsibilities?
    - Can you define and manage data management workflows and track progress of data governance activities?
- **Gain buy-in from the intended users of the technology before implementing it.** For a data governance tool to be effective, the staff using it must believe in the business value of the tool.
- **Ensure the implementation of the tool is accompanied by education, training, documentation and technical support.**
- **Ensure ongoing monitoring and maintenance of tools.**

12. Data Management

Where data governance sets the rules of engagement for how data-related decisions are made within an organisation through the creation of policies and processes, data management refers to the planning, execution and operation of these policies and processes.

As illustrated in the following figure, there are 8 core functions of data management which contribute to the effective governance of data:



Source: Adapted from DMBOK Data Management Framework

These functions are adapted from the Data Management Association (DAMA) Data Management Body of Knowledge (DMBOK). While each data management component is important, not all the functions must be included in the first phase of a governance program. For example, some programs will focus more on business definitions (Metadata) initially, while others may emphasise a single view of the customer (Master Data).

12.1 Data Quality Management

What is it?

An enterprise-wide process to manage and improve the quality of an agency's data is a key component of effective data management. Data quality management is a continuous process which involves managing data across the full data lifecycle, from its initial creation to its destruction. It involves the implementation of data quality standards and procedures to address and improve the accuracy, completeness, timeliness, relevance, consistency and reliability of the data.

Why is it important?

The outcome of decisions depends on the quality of the information used to make that decision. Poor data quality can result in poor decisions and unintended outcomes. High data quality can support an agency to achieve desired outcomes by ensuring decision-making is based on accurate and timely information. Data quality methods and procedures are essential to ensuring accurate data is available to decision-makers in a timely manner.

What good looks like:

- **Automated**: the quality of data is managed through automated tools that can automatically detect data quality issues and cleanse and enrich the data.
- **Lifecycle management**: the quality of data is proactively managed across the data lifecycle, from collection through to disposal.
- **Root-cause remediation**: problems with data quality are addressed at their root cause (e.g. fixing the problem at the source).
- **Enterprise-wide**: data quality management is regarded as a responsibility of all staff that have a role in handling data.
- **Standards-driven**: requirements are defined in the form of measurable standards and expectations against which the quality of data can be measured.
- **Monitored**: data quality requirements are enforced through clear monitoring, reporting and issues management processes.

How to achieve good practice:

- **Define data quality requirements for your agency that are relevant to your business needs**. This will ensure consistency across the organisation and help you determine which data to keep, which to get rid of, and which to correct.
- **Measure data quality levels** – a data quality assessment tells you how effectively data is meeting your business needs and stakeholders' requirements.
- **Create and implement a strategy for improving data quality** – this strategy should include:
    - Industry standards for available data
    - Organisational data standards
    - Timeliness for data availability
    - Data quality metrics
    - Goals for data quality metrics
    - Data quality rules for specific fields
- **Develop operational procedures and automated processes to improve data quality** – for example, the NSW Government Data Quality Reporting Tool can be used to understand the different dimensions of data quality and generate data quality statements. Data quality assessments should always be recorded in the metadata. Tools that automate data profiling are also available and can help your agency enrich large amounts of data.
- **Train staff with data responsibilities on data quality rules** – staff are responsible for ensuring that business rules or issues related to data quality are documented, developed and managed in a consistent way, in accordance with the agency's data requirements.
- **Monitor and report on quality levels of your data** – this supports the active management of data quality across the agency and enables the prioritisation of data quality improvement initiatives.

Relevant Standards:

- NSW Government Standard for Data Quality Reporting – the purpose of this document is to establish common principles and protocols for reporting on data quality, so that agencies can create simply data quality statements and users can easily evaluate whether shared or published data is suitable for re-use.

Useful resources:

- Data Quality Reporting tool – this tool is designed to support the NSW Government Standard for Data Quality Reporting. It guides you through a reporting questionnaire to generate a Data Quality Statement. All data should be accompanied by a data quality statement as it helps a user understand how the data can be used.
- ABS Data Quality Framework – NSW has adopted the Australian Bureau of Statistics (ABS) Data Quality Framework to describe the dimensions (or characteristics) of data quality. The framework can assist you with the development of statistical collections to produce high quality outputs.
- ISO 8000 Data Quality – this is the global standard for Data Quality and Enterprise Master Data. It describes fundamental concepts of information and data quality and how these concepts apply to quality management processes and quality management systems.

12.2 Metadata Management

What is it?

Metadata management means maintaining information about data to ensure both the users and systems:

- understand the meaning of data,
- know why data was created and for what purpose; and
- can find data easily when they need to.

By having high quality information that describes the information in data, as well as its storage and origin, staff can understand what the information is, what they can learn from it and how to find it quickly. Depending on the data, metadata may include the lineage, ownership, format, and any rules to be applied to the data.

Metadata management requires a consistent way to capture, manage and publish metadata information. This means controlling the creation of metadata by setting clear standards (and, where appropriate, adhering to well-established industry metadata standards), as well as implementing policies and procedures for metadata management and ensuring they are enforced across the organisation.

Why is it important?

Without metadata, it is very difficult for potential data users to know whether a dataset is available, where it is stored, what the data means, and how accurate it is. A key reason for duplicated data collection and re-work across government is the fact that repositories of what data has been collected are either inadequately maintained or do not exist. Therefore, implementing robust metadata management practices are required to ensure that data can be located, understood and used not only across the agency, but also by other agencies and non-government users.

What good looks like:

- **Valued**: the value of having managed metadata, and its role in improving data quality, is recognised across the organisation.
- **Standardised**: metadata conforms to relevant industry standards to enable data sharing and re-use across the public and private sector.
- **Accessible**: metadata is recorded and maintained on an accessible repository and is freely available at no additional cost with the provision of the dataset.

- **Assured**: the quality of metadata is assured, measured, monitored and improved.
- **Agreed**: changes to metadata are agreed and authorised with due consideration of impacts to other data management functions and business processes.

How to achieve good practice:

- **Identify the metadata associated with priority common data elements**. Determine the level of consistency of metadata for priority common data elements.
- **Measure current metadata effectiveness** and determine the level of consistency needed for efficient agency operations.
- **Define a minimum metadata standard for your agency** in consultation with agency stakeholders and ensure compliance with well-established industry standards.
- **Establish or improve metadata policies, rules, practices and roles** – this can be done by implementing a metadata adoption plan and implementation process across the organisation.
- **Educate staff on the value of metadata**, **as well as on access and use of metadata** – this may include education of staff on their respective metadata management responsibilities.
- **Create a single metadata repository where agency stakeholders can find information** – this can be done by bringing individual repositories together to develop a central (or federated) electronic database that is used to store and manage metadata.
- **Create feedback mechanisms** – to ensure that data users can provide input on the effectiveness of metadata and incorrect or out-of-date metadata.

Relevant standards:

- Metadata Online Registry (METeOR) – Australia's repository for national metadata standards for health, housing and community services statistics and information.
- ANZLIC Metadata Profile Guidelines – ANZLIC – these guidelines provide practical information to better understand and implement the ANZLIC Metadata Profile. The ANZLIC Metadata Profile defines the appropriate content of metadata for geographic information or spatial resources.

- AS ISO 23081.1:2018 – covers the principles that underpin and govern records management metadata.
- AS/NZS ISO 19115:2005 – provides a standardised metadata format for describing geographic information and services.
- AS/NZS ISO 15836:2016 – establishes a standard for cross-domain description and defines the elements typically used in the context on an application profile.

Useful resources:

- Metadata for records and information – NSW State Archives and Records provides a range of advice on metadata, including:
  - The minimum requirements for metadata for authoritative records and information
  - Principles for implementing metadata for records and information
  - What metadata for records and information can achieve
- National Archives of Australia Metadata for Interoperability Guide – this guide provides information on how to develop an organisational Metadata strategy, information on metadata harvesting tools and protocols, tips for building a metadata repository and links to relevant resources and standards.

12.3 Data Security and Privacy

What is it?

Data security and privacy management includes the policies, processes and procedures that are in place to ensure that data is kept safe and secure across all stages of the data lifecycle. Data security and privacy measures are implemented to protect agencies' critical, personal or otherwise sensitive data from unauthorised access and use, and ensure that data can move securely through the organisation. Adherence to privacy legislation, as well as customer and community privacy concerns, is paramount when considering data security and privacy management.

Why is it important?

Data can often contain personal, confidential or otherwise sensitive information that can have serious implications for both the populations the data is about and the organisations storing it. Good data governance practices across your organisation will ensure it is protected against misuse, interference, loss, or unauthorised access, modification or release. Serious physical, emotional or reputational harm to individuals may occur if data becomes compromised. Data breaches can also result in reputational damage and loss of public trust, as well as financial and legal ramifications.

What good looks like:

- **Compliance**: data is managed in accordance with relevant privacy legislation and NSW government and agency-specific security policies, procedures and standards.
- **Clear roles**: roles and responsibilities for authorising and overseeing safeguarding processes are clearly defined and access rights are assigned on a need-to-know basis.
- **Classified**: the safe handling requirements of data are known because each data asset is classified according to the NSW Government Information Classification, Labelling and Handling Guidelines.
- **Privacy-by-design**: privacy measures are built into the design and architecture of information systems, business processes and network infrastructure.
- **Minimised**: data creation and collection processes are designed to ensure that minimum personal information is collected.

- **Transparent**: agencies are transparent and accountable about the procedures used to protect personal data, including the choices made in balancing competing interests.

How to achieve good practice:

- **Define and communicate policies on privacy and security with staff** – ensure alignment with relevant legislation, policies and frameworks. For example, all staff must comply with the *Privacy and Personal Information Protection Act 1998 (NSW)*.
- **Assess current data security risk and define controls to manage risk** – risk analysis should include examination of unauthorised access; human factors such as accidental and intentional errors, omissions, destruction, misuse and disclosure.
- **Implement data privacy and security controls** – including privacy impact assessments (PIAs), privacy breach response procedures, clear arrangements for handling privacy complaints, multi-factor authentication, encryption, logging and monitoring procedures.
- **Training for staff on privacy, confidentiality and data security** – including education on existing industry-based standards for data handling, data minimisation and de-identification, the right for individuals to access and correct their personal information, as well as their role in ensuring data is collected and used only for the intended purpose(s).
- **Monitor, review and revisit data security measures** – continuous monitoring activities include control of IT system components, ongoing assessment of security controls, and auditing user access.

Useful resources:

- NSW Cyber Security Policy – outlines the mandatory requirements for sensitive and classified information.
- Information Classification, Labelling and Handling Guidelines – the Guidelines support the implementation of the NSW Cyber Security Policy. They provide guidance for the application of security classification to prevent government information assets from potential security breaches. This includes how to classify information and the protocols for handling and transmission of information.

- Making data safe for sharing guidance – provides guidance for NSW public sector agencies on how to make data safe (e.g. through data minimisation and de-identification) for sharing and public release.
- Five Safes Framework – provides guidance on how to develop safe data projects and manage disclosure risks according to five 'safe' components and allows data custodians to place appropriate controls on not just the data itself, but the manner in which data can be accessed.
- The IPC Public Interest Test – the Public Interest Test is the practical application of the *Government Information (Public Access) Act 2009* (GIPA Act) and it is designed to help you decide whether or not your data can and should be made open.
- IPC Information Governance Agency Self-assessment tool – enables agencies to conduct an assessment of their systems and policies that ensure their compliance with privacy and information and access requirements.
- Information and Privacy Commission NSW website – provides guidance on implementing privacy obligations under the PPIP Act and the IPPs and/or the HRIP Act and HPPs.

Relevant standards:

- ISO 27001 – sets of the international requirements for an Information Security Management System (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

12.4 Data Warehousing and Business Intelligence

What is it?

A Data Warehouse is a consolidation of data from a variety of sources that is designed to support and optimise organisational decision-making. Its main purpose is to consolidate data and provide readily available and easily accessible information to the business's decision-makers. Business Intelligence (BI) refers to a set of methods and techniques that are used by organisations to enable strategic decision-making. BI leverages technologies and tools that focus on reliable measurement of facts and business objectives to provide better insights to support evidence-based decisions.

Why is it important?

Fragmented, inconsistent and outdated data in multiple databases does not enable informed and strategic decision-making. Data warehousing and BI give business units a way to consolidate and process vast amounts of information and perform more advanced analytics. With appropriate data warehousing in place, systems have the right data available to perform more accurate analysis and get more value from BI and analytics programs. An agency that acts on knowledge gained from BI and analytics can improve operational efficiency and find better ways to innovate based on insights from data.

What good looks like:

- **Current**: the data warehouse supports appropriate information access and is designed to deliver up-to-date information to decision-makers.
- **Business goals:** the data warehouse serves agency strategic priorities and informs the selection of BI solutions.
- **Start with the end in mind**: the business priority drives the creation of the data warehouse content.
- **Once size does not fit all**: use the right warehousing and analytics tools and products for your specific purpose.

How to achieve good practice:

- **Understand your business needs** – start by consulting with stakeholders across the organisation to identify why your agency needs the warehousing and BI solution(s) and what objectives you are seeking to achieve.
- **Avoid one-stop-shop solutions** – while warehousing and BI solutions with all the features may seem enticing, focus on implementing solutions that meet your core business needs.
- **Don't overcomplicate the solution** – while there are endless data warehousing and BI tools available, it is important to focus on getting the basics right before you add additional requirements.
- **Use BI tools for their intended purpose** – rather than trying to find a tool that does it all, look for BI solutions that do something (or a few things) well. It's also important to find tools with user-friendly interfaces that meet the users' needs.
- **Consider how to make the transition easy for staff** – this can be done by ensuring there is a communication strategy for the transition, and that adequate training and guidance is available for staff who are expected to use the solution.

12.5 Reference and Master Data

What is it?

Reference and master data are data that provide a consistent, reliable record for all critical business data across the organisation. Master data can be defined as the “golden record” of critical information that the organisation relies on (e.g. customers, employees, locations, and products). Reference data is a type of master data that is more likely to change and that it less critical to the business. Agencies need to define and manage how master and reference data will be created, integrated, maintained, and used throughout the organisation. The challenges of this are determining the most accurate data values from among potentially conflicting data values and attempting to make that data available wherever needed.

Why is it important?

Definition and management of data assets used across an agency is necessary to meet strategic objectives, reduce risks associated with data redundancy, and reduce the cost of data integration. The management of master and reference data allows agencies to correct data inconsistencies across business units and systems and apply uniform business rules to enable sharing of data assets across agencies and government more broadly.

What good looks like:

- **Interoperable**: Master data and reference data is managed so that it is interoperable across business units and government agencies.
- **Standardised**: Master and reference data should be modeled according to agreed state, national and international standards so the data is represented appropriately.
- **Single view**: Master data is recorded and maintained on an accessible and, where possible, centralised repository to create a single view of the data.
- **Controlled**: changes to reference and master data are agreed and authorised with consideration of impacts to other business processes.

How to achieve good practice:

- **Identify and agree on data definitions** – this involves determining the most accurate data values from among potentially conflicting data values and getting agreement from different parts of the organisation.
- **Collect the master data into a central database** – this database should link to all participating applications.
- **Publish reference and master data** – ensure its use in all appropriate business intelligence and analytics reporting across the organisation, at all levels.
- **Establish maintenance policies and processes**

Relevant standards:

- ISO 8000-115 Data Quality – Part 115: Master Data – this is the global standard for Data Quality and Enterprise Master Data. It describes the features and defines the requirements for standard exchange of Master Data among stakeholders.

12.6 Data Storage and Operations

What is it?

Agencies must ensure data storage environments are secure, comply with relevant legislation, and enable information continuity, sharing and re-use. A number of laws and policies affect how NSW Government agencies can store their data. For example, NSW Government agencies must comply with the *State Records Act 1998* (NSW), which requires agencies to ensure appropriate records storage, maintenance, security and archiving. It is important to note that outsourcing storage does not lessen an agency's obligation to ensure information is stored appropriately.

Why is it important?

Due to its rapidly increasing volume, how and where agencies store their data is becoming increasingly important. Storage environments must be able to manage large volumes of complex data and to provide consistent levels of security, accessibility and functionality. To ensure the long-term continuity and accessibility of data assets, agencies need to find appropriate and secure storage environments that comply with legislative and regulatory requirements.

What good looks like:

- **Digital continuity**: storage environments enable information continuity by ensuring the preservation and maintenance of key data assets.
- **Retention and disposal:** storage environments ensure data is kept and disposed of in accordance with business requirements, protective security requirements, and legislative requirements under the State Records Act, PPIPA and HRIPA.
- **Best practice:** database standards and best practices are understood and applied.
- **Re-use:** storage environments that promote data re-use and integration are preferenced.
- **Migration, transition and decommissioning**: changes to storage environments are agreed and authorised to ensure that data of long-term value is transitioned to new environments or appropriately assessed in decommissioning arrangements.

How to achieve good practice:

- **Identify your agency's storage needs**. All agencies' storage needs will be different so it's important to identify and agree on these requirements.
- **Ensure alignment of business needs to the storage infrastructure**.
- **Ensure storage infrastructure complies with data retention periods** specified under the State Records Act and PPIPA.
- **Ensure the storage infrastructure selected is efficient and flexible**. This means that it is easy to search, query, and store the data.
- **Create and maintain a Data Asset Register/Inventory** that identifies high-value and high-risk data assets and their storage locations.
- **Manage and monitor effectiveness** of the storage infrastructure.
- **Ensure future planning for business continuity** by considering if the storage infrastructure is laying a foundation for future data initiatives and if it can be scaled as needed.

Useful resources:

- State Archives General Retention and Disposal Authorities – outlines the retention and disposal requirements for different types of information, as well as the requirements for storing records outside of NSW.
- NSW Government Cloud Guidance and Policy – provides practical steps to move services to a cloud. This includes information on preparation, contracting and managing, as well as considerations to note when moving to cloud.
- NSW Cyber Security Policy – agencies must abide by the Policy when procuring cloud services. The Policy outlines mandatory requirements to appropriately manage cyber security risks, including the requirement to identify agency 'crown jewels'.
- NSW Internet of Things Policy – provides practical guidance to help agencies design, plan and implement IoT solutions, including guidance on storage options for data generated by your IoT initiative.
- Australian Cyber Security Centre's Cloud Computing Security Considerations – provide detailed cloud security considerations, which include: maintaining availability and business functionality; protecting data from unauthorised access by a third party, the vendor's customers and by rogue employees.

- Government Data Centres Guidance – provides information on the benefits of government data centres and services, including secure data storage and access to services in the cloud.
- National Archives of Australia Outsourcing Digital Storage Guidance – provides advice on outsourcing digital storage, including key risks and consequences of offsite storage location. In addition, the Records Management Risk Assessment Template and the Checklist for Cloud computing and information management provide a helpful understanding of the potential risks and considerations associated with outsourcing storage of your agency's data.

12.7 Data Integration and Interoperability

What is it?

Data integration and interoperability is the ability of systems, organisations and people to exchange data between each other so that they can work together seamlessly, either in the present or in the future. Integration is the ability to consolidate data into consistent forms, either physical or virtual, and interoperability is the ability for multiple systems to communicate. Both are dependent on clear, shared expectations for the context and meaning of data across systems.

Why is it important?

Data integration and interoperability support the use and reuse of government data by allowing agencies to get data where it is needed, when it is needed, and in the form in which it is needed. Having integrated and interoperable data can assist agencies to make better decisions and to provide consistent, coordinated and more timely services by ensuring they have access to the right data at the right time. Lack of interoperability between systems means that government agencies often cannot share information effectively, which contributes to disjointed services, operational inefficiencies and poor citizen outcomes.

What good looks like:

- **Enterprise-wide**: data is stored in agency-wide enterprise architecture, where appropriate.
- **Standardised**: software and hardware conform to defined standards that promote interoperability for data, applications and technology.
- **Understood**: data users understand the meaning of exchanged information through the consistent use of metadata, master data and data quality standards.
- **User-friendly:** interfaces are flexible and generic enough to suit multiple uses.
- **Minimise replication:** data is linked rather than copied.
- **Modularity:** modularity of system design is maintained.

How to achieve good practice:

- Assess current state of interoperability to establish a strong understanding of your agency's business and data management environment
- Build future state vision that defines the requirements for creating new services and systems. Ensure requirements are defined across business functions to ensure the architecture supports the overall business strategy
- Undertake a gap analysis and quantify gaps between current and future state
- Planning and design of solutions to bridge gaps. Avoid boiling the ocean and focus on bridging gaps that are important for your business. Think quick-wins as well as long-term planning
- Implement frameworks, policies and standards and tools to support integration
- Monitor new processes for ongoing improvements

Useful resources:

- The National Archives of Australia has developed the following resources:
  - Interoperability key themes help you understand how interoperability is not just a technical fix, as it also relies on working with your information and data to align your business, security, legal and semantic needs.
  - Interoperability development phases will help you plan and implement solutions to address interoperability hurdles that are visualised in the interoperability scenarios.
  - Your results from using the Business System Assessment Framework (BSAF) can be used to identify:
    - the need to *integrate* business systems or to *migrate/export* data to address risks or gaps
    - system functionality to meet your information and data needs over time
    - what information and data is held in your systems and its value.
- The NSW Government IoT Policy also contains several sections related to interoperability.

12.8 Data Architecture

What is it?

Data Architecture defines information flows in an organisation, and how they are controlled. It relates to incoming data and determines how it is captured, stored and integrated into other platforms across the organisation. It involves understanding business objectives and the existing data infrastructure and assets, defining data architecture requirements, and shaping the enterprise data architecture to provide greater benefits to the organisation. The primary focus of data architecture is to integrate the existing applications and make them interoperable so data can be used across the organisation.

Why is it important?

Like many large organisations which have been in existence for a long period of time, government agencies have many legacy systems which use older technology or bespoke solutions to hold their data. These systems are often difficult to map out and connect with and require tremendous effort to support change.

What good looks like:

- **Aligned**: data architecture is aligned with the organisation's business strategy.
- **Comprehensive**: the data architecture minimises impact of information silos by combining data across the agency's business functions.
- **Integrated**: the data architecture provides a mechanism that documents the relationship among architecture components across domains and their alignment to agency and whole-of-government strategic goals.
- **Scalable**: the architecture can be applied to various organisational levels and scopes (i.e. whole-of-government, cross-agencies, agency, line of business, segments, capability, etc).
- **Flexible**: the architecture supports automation and is designed to meet changing business needs and new technology.
- **Standards**: the architecture adopts best-practice architectural design (such as Reference Architectures) to build and document common business and technical capabilities.

How to achieve good practice:

- **Assess current state architecture** of the organisation.
- **Define future state architecture** of the organisation, within the context of the strategic goals of an agency and its operating model.
- **Perform a gap analysis** between the current state and the future state.
- **Develop a roadmap or implementation plan** that contains a necessary set of actions to transform the organisation from the current state architecture to its target state.
- **Regularly report** on the effectiveness of the roadmap and implementation to the Data Governance Board or Committee.
- **Recruitment and retention of expertise in data architecture**, to guide agencies as they move away from legacy systems and siloed data towards integrated and consolidated data platforms.

Useful Resources:

- NSW Internet of Things Policy – provides practical guidance to help agencies design, plan and implement IoT solutions, including guidance on how to manage ICT infrastructure change when integrating or migrating new systems with legacy systems (see section 6.1.4)

Relevant standards:

- ISO/IEC 42010:2007 Systems and Software Engineering

13. Data Governance Checklist

This checklist outlines the best practice elements of an effective data governance program for NSW Government agencies. It is not exhaustive or mandatory.

13.1 Strategy and planning (see Module 4)

- ☐ The data governance program is tailored to the agency's specific business needs and strategic objectives, and has buy-in from key functions across the organisation
- ☐ An enterprise-wide data maturity assessment has been undertaken to identify the core data-related issues that need to be addressed to support desired business outcomes
- ☐ The data governance program is focused on solving a specific business problem and focus areas for the data governance program have been identified and prioritised according to their business value
- ☐ The strategy for data governance, as well as the outcomes of data governance initiatives, are frequently communicated to staff to ensure the vision is shared, accepted and sustained
- ☐ Metrics have been developed to assess whether the data governance initiatives are helping to achieve desired outcomes
- ☐ The data governance program is rolled out incrementally across the organisation

13.2 Organisational structures (see Module 5)

- ☐ A cross-functional senior executive data governance body has been established to oversee data governance decisions and activities across the organisation
- ☐ Working groups have been established to drive data governance projects and address specific data issues across the organisation
- ☐ The expectations and responsibilities of agency data governance bodies have been agreed to and communicated with staff across the organisation
- ☐ Working groups report on a regular basis to the overarching data governance body to ensure bottom-up, as well as top-down, information flows
- ☐ A visual representation of the agency's data governance structure exists that is accessible to all staff

13.3 Assigning roles and responsibilities (see Module 6)

- ☐ Roles and responsibilities have been assigned for all data assets and these responsibilities have been documented in a data catalogue

- Roles are appropriately matched with the responsible person's skills, expertise and delegation level
- The agency has a data governance framework or policy that specifies who is responsible for various aspects of the data
- Roles and responsibilities have been adapted to meet the agency's needs, organisational environment, culture, existing structure, and any limitations
- All data sharing agreements and service arrangements clearly specify data rights across the full data lifecycle
- A visual representation of the agency's data roles and responsibilities exist that is accessible to staff within the organisation

13.4 Leadership (see Module 7)

- Senior leadership display strong, explicit and ongoing commitment for data governance
- Senior leadership recognise and address data resource needs and infrastructure requirements to support data governance
- A senior executive decision-making body has been set up and senior leadership participate in decision-making on important opportunities and risk mitigation issues relating to organisational data assets
- Data metrics and goals have been incorporated into organisational plans and reporting
- A member or members of the senior executive (aka Chief Data Officer) has been appointed to lead and champion the organisation's data governance agenda

13.5 Data-driven culture (see Module 8)

- A targeted, multi-channel communications plan has been developed and implemented that aligns the agency's data initiatives with the organisation's overall objectives
- Staff have access to learning resources and training opportunities to grow their data literacy
- The effectiveness of data governance initiatives is measured and communicated to staff
- Each business unit across the agency has an assigned data leader to champion and engage staff on data governance initiatives
- Performance metrics have been developed and staff that demonstrate data-driven values and behaviours are recognised and rewarded
- A network exists for staff across the organisation to collaborate, lead and advocate for the agency's data agenda

13.6 Workforce skills and capability (see Module 9)

- A workforce skills and capabilities needs assessment has been completed
- A workforce strategy has been implemented to address data skills and capability gaps
- Staff have access to professional development opportunities (both face-to-face as well as online training) to build both foundational and specialised data skills
- Teams are either cross-disciplinary or staff with specialised data skills are spread across the organisation and can be leveraged by teams when required
- All staff have access to data governance resources and are aware of, and trained in, relevant data policies and procedures
- All role descriptions include the data skills and capabilities that are relevant to the data management activities that staff are expected to undertake

13.7 Technology (see Module 10)

- A current state technical capabilities and architecture assessment has been completed
- Areas for improvement and automation have been prioritised based on business needs
- Data governance policies and processes and data management workflows are automated (where appropriate)
- Technologies are compliant with privacy and security requirements and ensure the privacy and protection of data
- Implementation of new technologies is accompanied by education, training, documentation and adequate user support
- Technologies are well-integrated into the organisation’s culture and processes, have user buy-in, and support users to perform their roles more effectively and efficiently
- Technologies are monitored and regularly reviewed for improvement