NSW GOVERNMENT | Customer Service

NSW Data Governance Toolkit

Document number: Draft	**Version number**: 1.5
Date: Wednesday, October 16, 2019	

Contact details

Name: Data Analytics Centre, Program & Practice team, Department of Customer Service
Email: DataChampions@customerservice.nsw.gov.au

October 2019

Table of Contents

1. Introduction

1.1 Overview

The Data Governance Toolkit (the Toolkit) outlines a strategic and consistent approach for the effective governance of NSW Government data assets. It aims to provide NSW Government agencies with clear and consistent guidance on the key components of a successful data governance program, as well create a shared understanding of what good data governance looks like.

The Toolkit:

- sets out the principles that underpin effective data governance for the NSW Government;
- provides an overview of the legal, regulatory and governance environment in which agencies must operate;
- defines key data governance structures, roles and responsibilities;
- identifies the key organisational enablers required to drive data governance maturity; and
- outline the various data management functions that contribute to effective data governance.

1.2 Purpose

The overarching purpose of the Toolkit is to enhance NSW Government agencies' data capabilities and drive outcomes by providing a shared understanding of what effective data governance looks like.

While the use of 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 community expectations and well-established national and international standards;
- facilitate better interoperability between agencies by promoting whole-of-government policy and framework alignment; and
- build data governance maturity at both the departmental and all-of-government level.

1.3 Scope

Who does this Toolkit apply to?

The Toolkit applies to all NSW Government Departments and Public Service Agencies as well as all staff, contractors and other persons who, in the course of their work, contribute to or have access to NSW Government data.

Which data assets does the Toolkit apply to?

The Toolkit applies to all new and legacy data assets created, used and managed by the NSW Government. Application of the Toolkit to critical high-value data assets should be prioritised.[1]

1.4 Using this Toolkit

It is recognised that NSW Government agencies have different levels of data governance maturity. Many have already begun the journey of uplifting their data capabilities to help them achieve their agencies' vision and mandate.

The focus of this Toolkit is to provide some foundational steps agencies can take to improve their data governance capabilities, particularly those agencies with low data maturity. It also aims to provide clear and consistent guidance on the key components of a successful data governance program, as well as providing a shared understanding of what good practice looks like.

1.5 How was the toolkit developed?

This toolkit is being developed through a consultative and collaborative process with data users and subject matter experts across NSW Government. The NSW Government's Data Champions Network is playing a key role in its design and the Toolkit will benefit from ongoing input from Network members, as well as public sector agencies.

The Toolkit is a living document which will be reviewed and updated as necessary to ensure it is fit-for-purpose. If you have feedback on the Toolkit, please send it to DataChampions@customerservice.nsw.gov.au

[1] As it may be impractical for some public sector agencies to govern every data asset, focus should be on those that are deemed critical for business operations. Critical high-value data are data that best align to NSW Government strategic objectives, are central for the progression and development of the state, and/or are required for use and re-use across Government in support of various functions and services.

2. Background

2.1 What is data governance?

Data governance is a system of decision rights, accountabilities and processes aimed at improving the quality, availability, usability and security of an organisation's data. Data governance sets the rules of engagement for how data-related decisions are made within an organisation through the creation and enforcement of policies, processes, procedures and formalised roles and responsibilities, and structures.

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 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 on agency outcomes. It enables agencies to understand, manage and reduce risks around the data it holds, while extracting the maximum value from it.

2.3 What are the benefits of data governance?

Data governance must have a purpose for it to be beneficial. It should be established to help an agency achieve its strategic vision and it should clearly relate to business objectives. When data governance is aligned to agency's needs, it can deliver specific benefits across three areas: business value, efficiency and risk mitigation.

Business value	**Efficiency**	**Risk mitigation**
• Better decision making • Improved public trust and satisfaction • Reputation management • Better business value extracted from data • Simple access to information • Improved accessibility	• Reduction in duplication and waste created by information silos • Reduction in storage and document discovery costs • Reduction in the hours spent by employees locating information, interpret data and vet for quality issues.	• Avoid or mitigate information-related risk, including regulatory and legal risks • Improved ability to proactively meet compliance obligations • Understand key risk events, including the growing risk of cyber-attacks.

(Adapted from: Information Governance ANZ)

3. Guiding principles

Consistent with the NSW Information Management Framework, the Data Governance Toolkit is guided by the following information management principles:

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 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 spatially enabled**

   Quality data is of value to client, business and strategic objectives, and where relevant, spatial enablement allows for improves 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 person, 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**

   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.

4. Legal and Policy Context

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

4.1 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 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 to when collecting, holding, using and disclosing a person's health information.

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

  The 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 Act enables the sharing of data between NSW Government agencies, as well as the sharing of data 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.

4.2 Policies and other guidance

- ***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 principle facilitates 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 aligns with and expands on the 'Governance' section of the Framework.

- ***NSW Information Security 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.

4.3 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 issues by State Records NSW.

Standards specific to data management, for example data quality and metadata management, are included in the Data Management component of this Toolkit and are based on the internationally recognised Data Management Body of Knowledge guide.[2]

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

[2] The 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)

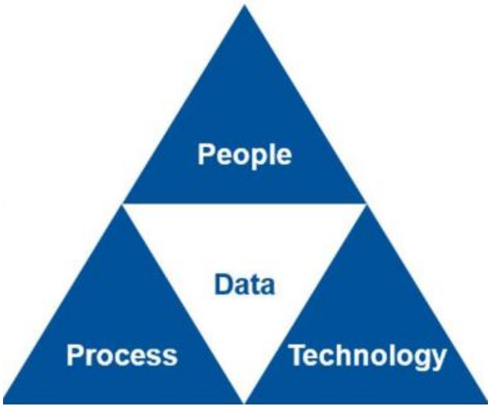
5. A model for strengthening data governance in NSW Government agencies

Outlined below is a model that has been designed to assist NSW Government agencies strengthen data governance maturity in their organisation. The model brings together all the components that are vital for any data governance program, regardless of the agency. To ensure best practice and alignment across NSW Government, agencies are encouraged to use this model as a basis for developing or strengthening their own data governance programs.

It is important to note that this model does not prescribe how agencies should implement their data governance program. Rather, it provides an organising framework for establishing a shared understanding of the broad scope of data governance activities to be undertaken, as well as a clear understanding of what good practice looks like.

What does the model cover?

The model defines four distinct levels of data governance activities, each of which is critical to achieving good data governance in agencies. The Model also aligns with the 'Golden Triangle' of 'People, Process and Technology' (with Data at the centre), which is often used to guide organisational transformation activities.



Source: Gartner 2017

The four levels of data governance activities are:

- **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. This is a foundational component of good data governance.
- **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. This is a foundational component of good data governance.

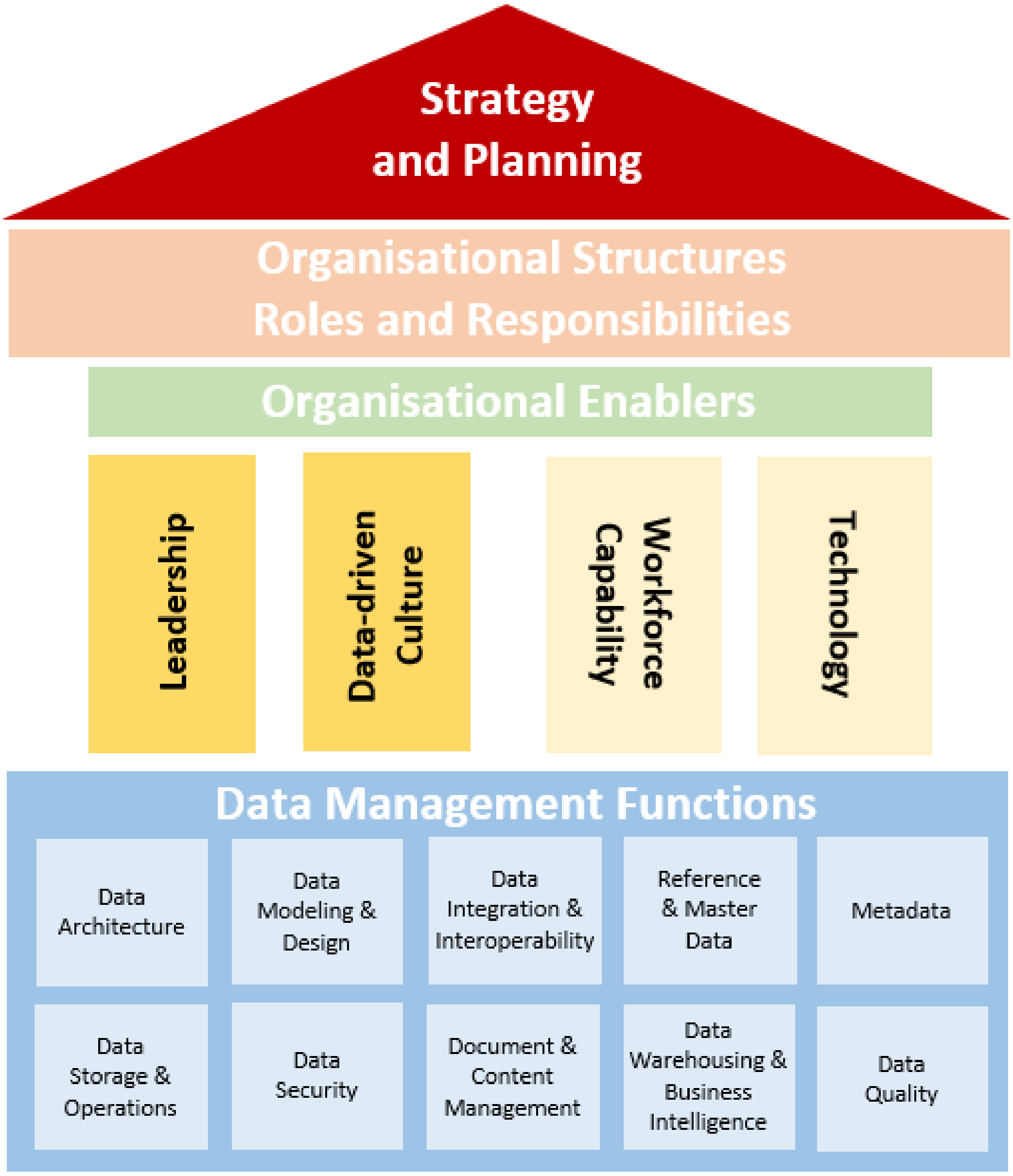
- **Organisational Enablers –** agencies ensure the organisational environment is an enabler of good data governance. This means ensuring there is a strong *motivation* (or 'will') to achieve good data governance by having sustained buy-in and investment from senior leadership, as well as fostering a 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. These organisational enablers collectively form the pillars that support good data management practices.
- **Data Management** – agencies ensure their data governance program has oversight of the ten core data management functions (e.g. data quality, storage, security, business insights etc.), as outlined by the Data Management Body of Knowledge Guide (DAMA-DMBOK).

Interpreting the Model

Each component of the Model, outlined in detail in the following sections of this document, 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, relevant standards, case studies and implementation tips.

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. In addition, the division of the Model into components is not intended to give the impression that the components can be dealt with independently. Many parts of the Model overlap and operate together, and data governance should be undertaken in a holistic way, incrementally and on an ongoing basis.

Figure 1: Draft Data Governance Model for NSW Government Agencies


Strategy
and Planning
Organisational Structures
Roles and Responsibilities
Organisational Enablers
Leadership
Data-driven Culture
Workforce Capability
Technology
Data Management Functions
Data Architecture
Data Modeling & Design
Data Integration & Interoperability
Reference & Master Data
Metadata
Data Storage & Operations
Data Security
Document & Content Management
Data Warehousing & Business Intelligence
Data Quality

5.1 Strategy and Planning

In the same way that agencies develop strategies to manage their other assets (ICT Strategy, Corporate Strategy, Workforce Management Strategy etc) it is important that agencies have an enterprise-wide strategy to manage and govern their data assets. This is vital for ensuring that data remains a valued, managed and business-aligned strategic asset. The strategy specifies the data governance program's vision, mission and business value and must align with the agency's overall objectives. The aim is to set the stage for treating data as a strategic asset, resulting in improved decision-making, enhanced user insights, and better outcomes for NSW citizens.

Why this is important

Having a clearly defined strategy for data governance provides an organisation with direction and ensures that siloed data activities are oriented towards a cohesive unified goal. It ensures that data assets are accounted for and that there is a pathway in place to maximize the use of those data assets, both in meeting their primary purpose, and to allow reuse for other authorised purposes such as data sharing or data integration.

What good looks like

- **Business-aligned**: the data governance strategy is tailored to the agency's unique vision, core goals, business needs and legislative and regulatory requirements
- **Future-focused**: the data strategy is flexible and accounts for future changes in the organisation, broader government policies and practice, industry technologies, and market forces
- **Measured**: all aspects of data are monitored, analysed and measured to ensure that the agencies data objectives are being achieved
- **Collaborative**: the strategy is developed iteratively with key stakeholders across different functions of the organisation
- **Prioritised**: the strategy is implemented gradually across the organisation and prioritised based on risk and value

How to achieve good practice

- Undertake a data maturity assessment to determine what information the agency needs to design, make and keep and where data requirements need to be built in to process, system, service, or contract design.
- Understand that data governance is not a one-off project and that it is an ongoing initiative that should be rolled out incrementally across the whole organisation. Start with a limited scope and focus on improving data governance in areas that will deliver clear business value.
- Develop and implement an enterprise-wide Data Governance Strategy that:
  - has input from all key functions across the organisation
  - aligns with the agency's overall mission and goals
  - is informed by the data maturity assessment and builds upon organisational opportunities while being cognisant of limitations
  - identifies, plans and manages key data assets and systems required to support business objectives and operations
  - defines and implements performance management, monitoring, analyses and metrics to report on data.

5.2 Organisational Structures, Roles and Responsibilities

5.2.1 Organisational Structures

People and organisational bodies are one of the most important aspects of Data Governance. This is because responsibility for protecting, maintaining and enhancing the value of enterprise data is ultimately assigned to them. All agencies should have a formalised data governance structure that involves key stakeholders across the organisation. An important component of this structure is having a cross-functional decision-making body, made up of senior representatives, that assumes overall accountability and responsibility for the strategic direction of data governance in their agency. This structure is agile (i.e. driven from the bottom-up) and informed by the needs of staff who work directly with the data.

Why this is important

Without a data governance structure, data flows in and out of many organisational silos, with nobody empowered to take responsibility for its entire journey through systems, databases and processes. This leads to siloed, inefficient and often contradictory data governance practices and in results in poor quality and under-utilised data. Having formalised data governance structure helps to break down silos and ensure data-related decisions and practices are aligned across the organisation. Assigning responsibility to committees or bodies for specific data functions and issues (e.g. privacy and security) also ensures that risks are minimised and the maximum value from the data can be derived.

What good looks like

- **Governed**: the decision-making structure includes a data governance body that is responsible for overseeing and driving high-level data-related decisions and activities
- **Cross-functional:** the decision-making structure includes stakeholders from across the organisation to ensure cross-functional decision-making
- **Agile:** staff who work with data are empowered to, and expected to, contribute to the corpus of knowledge about organisational data

- **Endorsement**: governance committees are responsible for endorsing and providing input on data governance activities
- **Engagement:** working groups are engaged to address agency-specific data needs such as data quality improvement, privacy and security
- **Contingent**: the data governance structure is not one-size fits all, and it is tailored to the agency's specific needs, strategic priorities, size, resources and its current level of data maturity

How to achieve good practice

□ Establish a cross-functional body of senior executives that has strategic oversight of data governance decisions and activities across the organisation

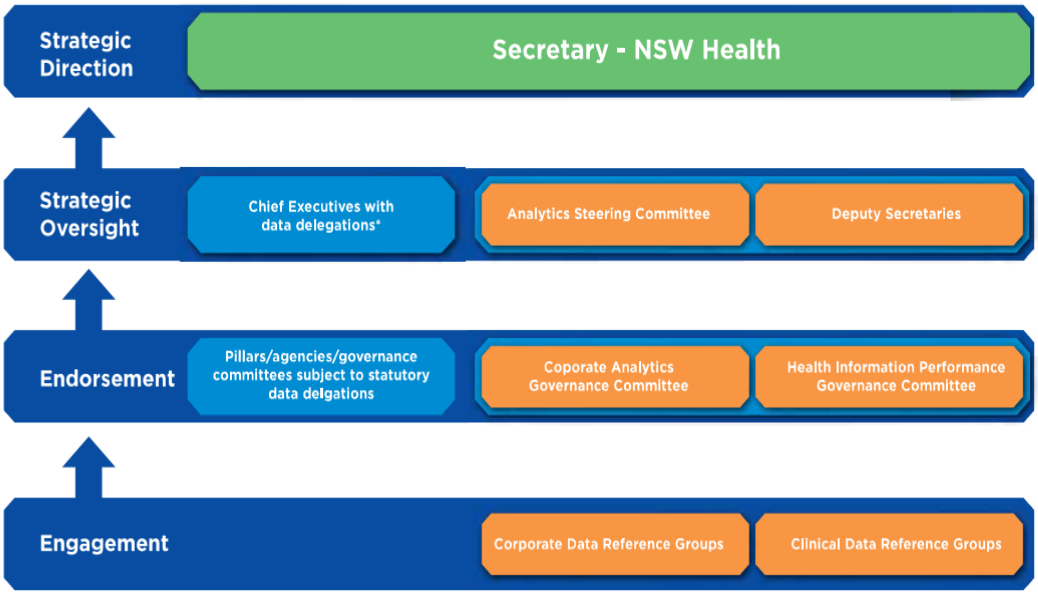
□ Establish decision-making authority (via working groups or committees) for key governance functions e.g. privacy, security, ethics, compliance

□ Ensure that working groups and committees report on a regular basis to the overarching data governance body

□ Develop a visual representation of your organisational data governance structures that is publicly available

Figure 2: NSW Health Data Governance Structure (2018)

Illustrated below is an example of NSW Health’s organisational data governance structure. The reason why it has been included is because it reflects several of the good practice principles mentioned above.


Strategic Direction
Secretary - NSW Health
Strategic Oversight
Chief Executives with data delegations*
Analytics Steering Committee
Deputy Secretaries
Endorsement
Pillars/agencies/governance committees subject to statutory data delgations
Coporate Analytics Governance Committee
Health Information Performance Governance Committee
Engagement
Corporate Data Reference Groups
Clinical Data Reference Groups

5.2.2 Roles and Responsibilities

For data governance to be successful, agencies need to clearly define the people who will be responsible for the data. Assigning roles ensures there are people within the organisation who are responsible and accountable for the data and that data is appropriately managed throughout its lifecycle.

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. A NSW Government agency may delegate its responsibility for the day-to-day creation and management of the data to another organisations, but the originating agency will continue to have overarching accountability for the integrity and security of the data. These responsibilities are usually delegated to Secretaries or agency heads under various pieces of NSW legislation.

What does good look like

- **Assigned**: data roles and responsibilities are clearly defined and formalised across the organisation
- **Aligned**: data roles and responsibilities are defined consistently across the organisation and, where appropriate, align with the NSW Data Governance toolkit (refer to Figure 2)
- **Appropriate**: data roles are appropriately matched with the responsible persons skills, expertise and delegation level
- **Understood**: all staff understand the data governance responsibilities associated with their role and are familiar with relevant policies and procedures
- **Specified**: data sharing agreements and service arrangements clearly specify data rights, including whether responsibilities for the data will be transferred to a third party

How to achieve good practice

□ Formalise data roles where they already exist and avoid assigning responsibility to anyone who is not already undertaking the role in their day-to-day work

□ If your agency lacks internal data expertise, recruit staff with specialised data skills and ensure position descriptions include information about their data responsibilities

□ Develop a visual representation of your organisations data governance roles and responsibilities that is freely accessible to staff within the organisation, as well as other agencies

□ Develop resources that provide clear guidance on data roles and responsibilities, including reporting lines, that align with the table on the following page.

The table below is adapted from the NSW Ministry of Health's Data Governance Framework and summarises the key data governance and management functions that are recommended for adoption by agencies to ensure data assets are managed appropriately. These functions may or may not reside within the remit of specific roles, and in some cases individual roles may involve more than one of these data governance functions.

While is it recommended that agencies assign these functions to separate roles (in order to maintain reasonable separation of authority and minimise opportunities for conflicts of interest), it is recognised that resourcing constraints may limit the ability of many smaller agencies and organisations to separate these functions.

Function	Main Responsibilities
Accountable Accountable Executives have **accountability** for the data and are generally the Head of Agency, however this role is often delegated to the Cluster Chief Information Officer or other designated Senior Executive. This role is typically referred to as the Data Sponsor or 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 or system • Monitor the performance of data governance responsibilities and identify improvements • Delegate responsibilities for decisions and tasks to Responsible Executives.
Responsible 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 data assets held and formally register roles and responsibilities for those • Approve the information security classification of data assets to ensure integrity • Determine the conditions for appropriate use, sharing and distribution of that asset • Nominate the Data Manager for data assets and ensure responsibilities are fulfilled

Operational management Data Managers are generally business managers, process owners or subject matter experts with the greatest operational stake in the content of the data asset and with operational (**frontline**) data management responsibilities. 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 • Approve access requests and data release according to policies and procedures • Manage the data asset in compliance with relevant legislation, policies, standards and any conditions specified by the data sponsor • Monitor compliance against data asset business responsibilities • Work with stakeholders to develop and maintain metadata including a data dictionary, business rules and guide for use • Coordinate stakeholder engagement and input into the business requirements for the data asset • Provide advice to the Responsible and Accountable Executives on the management of the asset • Provide feedback to data creators/ suppliers in relation to data quality issues
Data Creator / Supplier 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.	• Ensure data is recorded or collected according to agreed data standards • 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 it was created) • Ensure processes are in place for the ongoing maintenance of the data • Comply with legislation, policies and standards • Comply with terms and conditions associated with consent to collect data
Data User Data Users can be anyone, inside or outside of government, who uses any of the government's data assets.	• Understand the data accessed and ensuring it is fit for its intended purpose • Ensure data is recorded or collected according to data standards • Report errors regarding data they receive in a timely manner • Ensure security & privacy are maintained whenever data is accessed • Report any break or suspected breaches • Comply with legislation, policies and standards • Obtain approval from the Accountable Executive or delegated authority for public release of data • Comply with terms and conditions associated with approval for access to data

5.3 Organisational enablers

Data governance doesn't exist in a vacuum. A mix of organisational enablers are required to ensure that an agencies data is managed effectively and transformed into meaningful information. Organisational enablers can be grouped into those that leverage the motivations (i.e. the 'will') of staff and leadership, and those that leverage the capabilities (i.e. the 'skill') of staff and technologies to enable good data governance:

- **Motivation (the 'Will'):**
  - Leadership, sponsorship and investment
  - Data-driven culture

- **Capabilities (the 'Skill')**
  - Workforce skills and capability
  - Tools and technologies.

5.3.1 Leadership, Sponsorship and Investment

Sustained leadership, advocacy and funding from top-level leadership is pivotal in delivering a strong 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. All levels of leadership should play a key role in driving the data agenda of the agency and facilitating collaboration across business areas to ensure data-related decisions and activities are aligned with the agency's overall vision and business objectives.

Why this is important

Without sustained executive leadership and sponsorship, it is almost impossible to obtain the funding, resources, support and alignment necessary for successful data governance. In addition, maximising the value of data usually requires some level of transformation within an agency. For this reason, leadership and change management are critical and should be led by individuals that are sufficiently senior to exert influence within the organisation and build positive relationships.

What good looks like

- **Executive 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

How to achieve good practice

□ Develop and deliver training in strategic 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

□ Commission several high-value data governance projects to demonstrate commitment

□ 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

□ Ensure your agency has appointed a member of the senior executive (aka a Chief Data Officer) to lead and champion the organisation’s data governance agenda

5.3.2 Data-driven Culture

Creating an organisational culture that values data is a crucial success factor for an organisations data governance program. A data-driven culture means shifting the mindset of employees so they are motivated to manage and use data effectively. It involves raising awareness, knowledge and acceptance of an agencies data objectives, embracing openness and data sharing and encouraging risk taking for innovation.

Why this is important

When data is not regarded as a strategic asset by staff across the organisation, data quality degrades, silos proliferate, and inefficiency, poor decisions and unintended outcomes reign. In many respects, a data-driven culture will follow naturally if there is strong commitment from senior leadership, staff are data literate, and data capabilities are spread 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 of the organisation, and at all levels of the organisation.

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:** data champions are celebrated by all levels of leadership and encouraged to share their knowledge and expertise across the organisation
- **Collaborative:** all parts of the organisation are engaged on enterprise-wide data governance initiatives and input from relevant stakeholders is incorporated from day one
- **Business-enabler:** staff have a strong understanding how data governance can help them do their jobs more effectively and deliver real value for citizens and the organisation
- **Ethical:** robust data governance and management practices are considered by staff as an ethical imperative rather than a compliance requirement

How to achieve good practice

- Develop and deliver learning opportunities and resources to raise data skills for all data users, including in data storytelling and visualisation

□ Align data governance with the agencies overall vision and objectives by communicating how data governance supports and drives desired outcomes

□ Focus on generating quick wins that will enable staff to see and experience the tangible benefits of using data

□ Include all functions of the organisation in the planning and creation of data governance strategies

□ Identify data champions and set up a community of practice for staff across the organisation who can lead and advocate for the agency’s data agenda

□ Establishing a strong internal communication channel to engage with staff on data governance decisions and initiatives

□ Measure the progress of your data governance initiatives so the benefits of data governance for the organisation and the community are clear

5.3.3 Workforce skills and capability

Data skills and capability are critically important for building data governance maturity. Agencies need to be supported by a workforce that has the skills and capability to manage data effectively and extract the most value from the data. This means ensuring all staff have a foundational level of data literacy and there are staff spread across the organisation with specialised data skills and capabilities. Data literacy includes the ability to identify, locate, interpret, and evaluate information, and communicate key insights to drive action. Skills and knowledge in publishing, linking and sharing public sector data are also critical in ensuring data is managed appropriately, in line with legal requirements and community expectations.

Why this is important

Data skills and knowledge are essential for all NSW Government employees to support evidence-based, informed decision-making, whether in policy development, program management or service delivery. These skills also assist in improving operational efficiency, more efficient resource allocation, and improved engagement with stakeholders. 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.

What good looks like

- **Data-literate**: all staff have a foundational level of data literacy
- **Specialised**: there are staff spread across the organisation with specialised data skills that can be leveraged when required
- **Development-focused:** agency leadership support 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**: all staff have access to data governance resources and are aware of, and trained in, relevant data governance policies and procedures

How to achieve good practice

- Harness existing skills capabilities within the organisation and establish multidisciplinary, cross agency teams to achieve skill-sharing and optimal project outcomes.
- Invest in the development and recruitment of staff with specialised high level 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:[3]
  - **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
- If there is a lack of high-level data expertise in and across project teams, engage experts during the stage when the specific skill is required. To engage experts:
  - ▪ Look within your agency for internal expertise
  - ▪ Look broader within NSW Government for expertise
  - ▪ Engage academics, industry associations or other organisations for expertise.
- Provide employees with foundational and specialised data skills training and learning resources. For self-guided learning resources, refer to the NSW Data Skills – Learning Resources and the APS Data Literacy Learning Guide

[3] Commonwealth of Australia (2016) Department of the Prime Minister and Cabinet, Skills and Capability in the Australian Public Service.

5.3.4 Tools and technologies

With the increasing speed, volume and complexity of data, it is nearly impossible for humans to manage data appropriately and in a timely manner. Although technology is not a solution on its own, it can be a significant enabler of data governance by simplifying and automating policies and processes. For example, the right tools can automatically detent a piece of personal data like a security number in a dataset and trigger an alert. Tools can also be used to manage and improve the quality of the data with validation, data cleaning and data enrichment. In addition, technologies such as identity management systems and permission management capabilities simplify and automate key aspects of data governance.

Why this is important

Data governance systems that rely heavily on humans to profile, validate and monitor the data, face higher risks than systems that automate data governance processes. Despite good intensions, human error almost always creeps into data processes. These errors can lead to false, fragmented and duplicated information. Automated data governance tools help eliminate this problem by, for example, efficiently managing access controls, workflow processes, and improving data quality through the automated detection of data quality issues. Technology solutions can also increase efficiency by freeing staff from manual, inefficient process steps to an increased focus on the data.

What good looks like

- **Automated**: data governance policies and processes and data management workflows are automated
- **Enterprise-wide:** technologies break down organisational data silos and are implemented enterprise-wide
- **Interoperable:** tools and technologies support standard formats allowing interoperability across the organisation
- **Secure:** tools and 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

How to achieve good practice

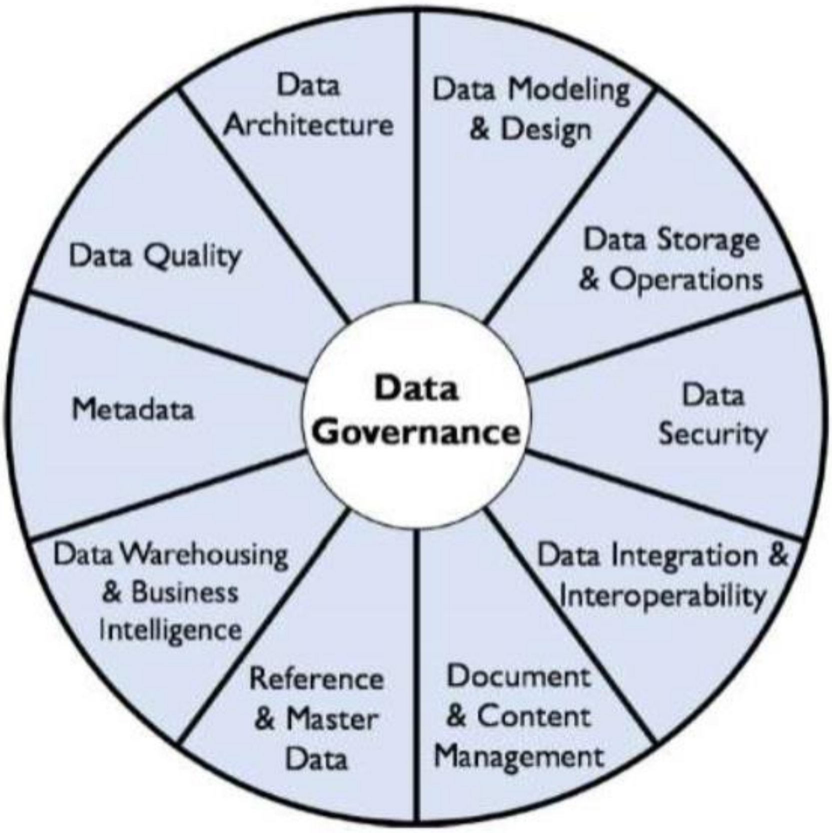
- Assess the current state technical capabilities and architecture of the organisation and identify and prioritise focus areas for improvement
- Identify opportunities to automate data governance policies and processes
- Look for open source, scalable tools that are easy to integrate with the agencies existing environment
- When selecting technologies, agencies should consider:
  - Can it identify and track common create, read, update and delete activities for data elements?
  - Can it provide effective data quality management (i.e. rules, profiling, reporting)?
  - Can it perform data movement, data lineage views, and positioning?
  - Does it provide metadata support for document classification and document lifecycle management?
  - Does it assign and manage governance roles and responsibilities?
  - Does it define and monitor service-level agreements, issues and activity statuses?
  - Can you define and manage data management workflows and track progress of data governance activities?
  - Can you monitor business strategies and plans, and calculate the business value of data?

In many cases, you won't find a single tool that meets all these criteria. You might instead opt for a series of connected data governance tools that provide a complete data governance pipeline – from data modeling, through integration and transformation, to reporting and visualization.

5.4 Data Management

Where data governance defines how data should be accessed and treated in an organisation, data management refers to the execution of data governance policies and processes.

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


Data Architecture
Data Modeling & Design
Data Quality
Data Storage & Operations
Metadata
Data Governance
Data Security
Data Warehousing & Business Intelligence
Data Integration & Interoperability
Reference & Master Data
Document & Content Management

(Source: DMBOK Data Management Framework)

These functions are adapted from the Data Management Association (DAMA) Data Management Body of Knowledge (DMBOK). While each is critical to data governance, not all of the functions must be included in the first phase of a governance program. Some programs will focus more on business definitions (metadata) initially, while others may emphasise a single view of the customer (Masterdata).

5.4.1 Data Quality Management

An enterprise-wide process to manage and improve the quality of the organisation’s data should be established. Data quality management includes the standards and procedures on the quality of data and how it is monitored, cleansed and enriched. Data quality standards and procedures need to address the accuracy, completeness, timeliness, relevance, consistency and reliability of data.

Why is this important

The outcome of government policy, program and service delivery decisions depends on the quality of the data used. Poor data quality exposes the government to ineffectiveness, the risk of poor decisions, and unintended outcomes. High data quality can contribute to achieving desired outcomes to effective decision-making based on accurate and timely information. Data quality methods and procedures are essential to ensuring accurate data is available in a timely manner to decision-makers.

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 managed across the data lifecycle, from collection or procurement 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**: maintaining data quality is regarded as a requirement for all staff
- **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

- Create and implement a data quality strategy – 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
- Define data quality requirements
- Measure current data quality levels – this can be done with the help of profiling, querying, reporting tools, user interviews, logs etc.
- Develop operational procedures and automated processes to improve data quality
- Train users on data quality rules
- Monitor and report data quality levels and findings – this can be done using dashboards that record number/percentage of duplicates, percentage of data changed, percentage of data cleansed, percentage of missing values, comparison between quality load vs. current data load.

Relevant Standards (not exhaustive)

- 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.

Helpful 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 hose these concepts apply to quality management processes and quality management systems.

5.4.2 Metadata Management

Metadata management includes maintaining information about enterprise data such as its description, lineage, usage, relationships and ownership. Effective data governance requires a way to capture, manage and publish metadata information. This means controlling the creation of metadata by setting clear enterprise-wide standards, policies and procedures for metadata management and ensuring they are enforced.

Why is this important

Metadata plays an important role in ensuring users and systems understand the meaning of the data. By having high quality information that describes the information in data, as well as its storage and origin, humans understand what the information is, what you can learn from it and how to find it quickly.

What good looks like:

- **Valued**: the intrinsic 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 exchanges
- **Access**: metadata is recorded and maintained on an accessible repository and is freely available at no additional cost with the provision of the dataset
- **Quality**: 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

□ Define a minimum metadata standard for your agency – this can be done through the application of industry standards, data dictionaries, naming standards, code values, and metadata entry tools etc.

□ Measure current metadata effectiveness – this can be done by assessing your organisations metadata to see if it meets the standards for a specific process.

□ 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 data custodians, stewards and specialists on their respective metadata management responsibilities.

□ Establish and manage metadata repositories – this can be done by bringing individual repositories (also referred to as registries) together to develop a central 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 (not exhaustive):

- Metadata Online Registry (METeOR) – Australia's repository for national metadata standards for health, housing and community services statics and information.
- ANZLIC Metadata Profile Guidelines – ANZLIC – this guideline provides 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.
- ISO/IEC 11179 – provides a standardised metadata format to describe and represent data to make it easier to understand the meaning and content of data.
- 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.

Helpful resources:

- 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.

5.4.3 Data Security

Data security includes policies, processes and procedures to protect the privacy and confidentiality of data at all stages of the data lifecycle. These actions require adopting security standards in the technical systems, as well as policies for staff. The best practice for applying these policies is to develop a role-based model where access rights are granted to roles and groups, and individuals are assigned to one or more roles or groups. Special care should be taken for regulatory requirements and privacy concerns. Ensuring the right people have access to the right data is key to effective governance.

Why this is important

Data can often contain private and sensitive information that can have serious implications for both the populations about whom data are being shared and the organisations sharing the data. Good data governance practices across your organisation will ensure it is protected against misuse, interreference, loss, unauthorised access, modification or release.

What good looks like

- **Compliance**: data is collected, stored, used & disclosed, archived & disposed in accordance with relevant privacy legislation and privacy and security policies, procedures and standards.
- **Clear roles**: clearly defined responsibilities for authorising and overseeing safeguarding processes and clearly documented and appropriate assignment of access rights across the organisation.
- **Classified**: the safe handling requirements of data are known because each data asset is classified appropriately according to the NSW Government Information Classification, Handling and Labelling Guidelines.
- **Proactive management**: data security is managed proactively, dynamically and collaboratively with relevant internal and external stakeholders
- **Privacy-by-design**: privacy measures are built in to the design and architecture of information systems, business processes and networked infrastructure
- **Needs-based**: 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 – these must align with applicable legislation, policies and frameworks.

□ 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, disclosure and negligence; and external threats such as trojans, malware and spyware.

□ Implement data security controls and procedures - including privacy impact assessments, privacy breach procedures, clear arrangements for handling privacy complaints, user identification management, multi-factor authentication, encryption, logging and monitoring procedures etc.

□ Training for staff on privacy, confidentiality and data security – including education on existing industry-based standards for data handling 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 configuration management and control of IT system components, ongoing assessment of security controls, and management of an audit log and status reporting.

Helpful resources

- NSW Cyber Security Policy – includes requirements for sensitive and classified information.
- Information Security Classification, Labelling and Handling Guidelines – the Guidelines support the implementation of the NSW Government Digital Information 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 for sharing and public release.
- The IPC Public Interest Test – The Public Interest Test is the practical application of the Government Information Public Access Act (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.
- IPC Privacy Governance Framework

5.4.4 Data Warehousing and Business Intelligence

A Data Warehouse is simply a consolidation of data from a variety of sources that is designed to support strategic and tactical decision making. Its main purpose is to provide a coherent picture of the business at a point in time. Business Intelligence (BI) refers to a set of methods and techniques that are used by organizations for tactical and strategic decision making. It leverages technologies that focus on counts, statistics and business objectives to improve business performance.

Why this is important

Fragmented, inconsistent and outdated data in multiple databases does not permit good strategic and tactical 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 data governance 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 business intelligence and analytics can improve operational efficiency, find better ways to innovate based on insights from data, and drive better outcomes.

What good looks like:

- **Single-view:** data is consolidated from disparate sources into an enterprise-wide data repository to achieve a single view of the data
- **Current**: data repository supports real-time or near real-time information access and is designed to deliver up-to-date information to decision-makers
- **Business goals:** data repository serves organisational priorities and informs solutions
- **Outcomes-focused**: business priorities drive the creation of data repository content
- **Start with the end in mind**: the business priority and scope of end-data-delivery drives the creation of the data repository content.
- **Once size does not fit all**: use the right BI tools and products for your purpose

How to achieve good practice

□ Understand requirements

□ Define and maintain BI design

- Implement BI solutions
- BI activity monitoring

5.4.5 Reference and Master Data

Reference and Master data is the collection of generally non-transactional data that gives context to transactions, and provides connection points between and among related data in differed records, files, tables and other formats. 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 this important

Definition and management of the critical data assets used across an agency is necessary to meet business 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 applications and apply uniform business rules to enable sharing of data assets across agencies and government functions.

What good looks like

- **Shared**: Masterdata and Reference Data is managed so that it is interoperable across business units and agencies
- **Standardised**: Master and reference data should be modeled according to agreed state, national and international standards so the data is represented appropriately.
- **Centralised**: Masterdata is recorded and maintained on a central repository creating a single view of the data
- **Controlled**: changes to Reference and Masterdata are agreed and authorised with due consideration of impacts to other data management functions and 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 & Masterdata – 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.

5.4.6 Data Storage and Operations

Agencies must ensure data storage environments are secure, appropriate 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)* requires agencies to ensure appropriate records storage, maintenance, security and archiving. Outsourcing storage does not lessen an agency’s obligation to ensure information is stored appropriately.

Why this is important

Due to its rapidly increasing volume, how and where agencies store their data is becoming more important than ever. 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 for classified and unclassified information, and legislative requirements under the State Records Act and PPIPA
- **Best practice:** best practices including database standards and 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 migrated or transitioned to new environments or appropriately assessed in decommissioning arrangements

How to achieve good practice

□ Assessment of organisational architecture needs

□ Alignment of business needs to enterprise architecture

□ Manage and monitor effectiveness of enterprise architecture

□ Future planning for business continuity

Helpful resources

- NSW Government Cloud Policy and Guidance – provides practical steps to move services to a cloud. This includes information on preparation, contracting and managing, as well as considerations to note when mobbing 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.
- Australian Cyber Security Centre's Cloud Computing Security Considerations – provide detailed cloud security considerations, which includes: maintaining availability and business functionality; protecting data from unauthorised access by a third party, the vendor's customers and by rogue employees.
- Government Data Centers Guidance – provides information on the benefits of government data centers 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.

5.4.7 Data Integration and Interoperability

Data integration and interoperability means the ability of systems, organisations and people to exchange and use data without knowledge of the inner workings of the collaborating systems (or organizations). Integration consolidated data into consistent forms, either physical or virtual. Interoperability is the ability for multiple systems to communicate. Data integration and interoperability are both dependent on clear, shared expectations for the context and meaning of data across systems. They 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.

Why this is important

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, adverse events, inefficiencies and poor citizen outcomes.

What good looks like:

- **Government-wide**: data is stored in whole-of-government or 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, Masterdata 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 stare
- □ Planning and design of solutions to bridge gaps. Avoid boiling the ocean and focus on bridging gaps that are critical to make your business work and operate. 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

Helpful 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.
- Minimum metadata supports a standards-based approach to sharing information and data.

5.4.8 Data Architecture

Data Architecture defines information flows in an organisation, and how they are controlled. It looks at 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 prime focus of data architecture is to integrate the existing applications and make them interoperable.

Why this is important

Like many large organisations which have been around for a while, government agencies have a lot of legacy systems which use older technology or bespoke solutions to hold their data. These systems are often difficult to map out, 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 architecture eliminates information silos by combining data across the agencies business functions and across the agency as a whole
- **Integrated**: the architecture provides a mechanism that documents the relationship among architecture components across domains and their alignment to agency and whole-of-government strategic goals
- **Accessible**: the architecture provides the right interface (e.g. web-based dashboards, BI, SQL queries etc) for users to consume the data
- **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 & new technology
- **Standards**: the architecture adopts best-practice-based architectural design (such as Reference Architectures) to build and document common business and technical capabilities.

How to achieve good practice:

□ Assess current state (baseline) architecture of the organisation

□ Define future state (target) architecture of the organisation, within the context of the strategic goals of an agency and its operating model

□ Perform gap analysis between current state and future state

□ Develop an Architecture 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 centrally-stored data platforms

Relevant standards:

- ISO/IEC 42010:2007 Systems and Software Engineering – Architecture Description