NSW Infrastructure Data Management Framework (IDMF)

NSW
GOVERNMENT

Table of contents

Table of figures

NSW Infrastructure Data Management Framework (IDMF)

1 Introduction

The NSW Government builds, owns and manages a significant portfolio of major infrastructure assets. The planning, design, construction and operation of these assets results in the creation, procurement and use of increasingly valuable data relating to the infrastructure portfolio. This data and information is a state asset that needs to be effectively managed across the lifecycle of the infrastructure assets.

The Infrastructure Data Management Framework (IDMF) is a set of guidelines, procedures and standard approaches to support consistent management of infrastructure data across the NSW Government sector. The IDMF is aligned with the NSW Information Management Framework (IMF), which provides more general guidance on the management of government data and information.

Broad adoption of the principles and guidance of the IDMF will ensure that NSW has a coordinated, standardised and trusted framework to harness infrastructure data to better plan and operate the State's infrastructure systems. It provides guidance on the generation or collection, curation, sharing, archival and disposal of the State's infrastructure data.

1.1 Vision and Objectives

The vision for the IDMF is to:

Establish a coordinated, shared, and standardised approach within NSW Government for the management of infrastructure data.

This vision is supported by several key objectives, including to:

- improve access to NSW Government infrastructure data and information
- improve collaboration and sharing of service and infrastructure data and information managed by multiple information stewards and custodians, across the asset lifecycle
- improve service and whole of life infrastructure investment decisions informed by data
- improve the ability of agencies to meet and document statutory and legislative compliance requirements with respect to infrastructure data management
- protect critical infrastructure through appropriate management of sensitive infrastructure data
- capture lessons learnt and best practice on data management from NSW Government agencies and service providers.

The IDMF provides guidance on process and data requirements to support agencies in adopting this framework. It relies on the NSW Open Data Policy and encourages the use of Data.NSW integrated platforms and services to publish and share data in near to real time.

Adoption and implementation of the IDMF will assist agencies and contracted service providers to:

- Manage infrastructure data and information in a secure, structured and consistent manner using recognised standards
- Enable informed decision making in relation to planning, delivery and management of safe, sustainable and integrated infrastructure by having the right data and information available and accessible at the right time
- Ensure that decision makers use fit for purpose data to support evidence-based decision making to balance whole of life cost, risk and asset performance.
- Understand infrastructure investment outcomes and place based interdependencies across clusters

The IDMF supports the creation and management of digital twins for infrastructure assets to enable smart infrastructure and smart places. Adoption and implementation of the IDMF will be measured against the objectives above.

1.2 Principles

Application of common, open standards will enhance usability of infrastructure data, including digital twins, and maximise benefit to users. Management of information and data to agreed principles leads to better outcomes throughout the infrastructure lifecycle including optimisation of resources and better service delivery. The following principles have been used to guide the development and application of the IDMF:

Objective	Public Good	Infrastructure data should deliver public good
	Value	Infrastructure data should provide ongoing value and insights to inform planning, development, operation and maintenance of infrastructure across the asset lifecycle
Function and Form	Quality	Infrastructure data should be reliable, consistent and known quality
	Adaptability	Infrastructure data should be flexible and scalable to allow adaptation to new technology and societal needs
	Openness	Infrastructure data should be as openly available, transparent, authoritative, accessible and discoverable as possible to maximise value and reuse
Governance and Accountability	Security & Privacy	Infrastructure data should be governed by processes that ensure privacy by design, and facilitate security and privacy-preserving role-based access
	Curation	data should be curated by processes that allocate responsibilities, ownership, monitoring and management
	Standards	Infrastructure data should meet consistent agreed standards (open where feasible) to enable interoperability
	Federation	Infrastructure data should be able to be federated to enable an interconnected eco-system of data environments supported by custodians

Table 1: Principles

These principles should be used as guidance by agencies to implement and adapt the IDMF to suit the needs of their customers and internal and external stakeholders, and to support strategic outcomes. The principles draw on the UK's Centre for Digital Built Britain's Gemini Principles, the ANZLIC Principles for Spatially Enabled Twins of the Natural and Built Environment in Australia and the F.A.I.R. Principles (Findable, Accessible, Interoperable, Reusable). These principles have been adapted to NSW needs and priorities to ensure that agencies and their users can safely and effectively find, read, use, share and reuse infrastructure data.

1.3 Readers Guide

Varying audiences will find value in different sections of the IDMF. The introductory sections will be of value to all readers to provide important contextual and conceptual links to state strategies, policies and frameworks, while the later sections provide greater detail on key topics.

Role	Sections
Senior executives	Executive Summary, Introduction, Overview, Key Concepts, Organising the organisation, Next Steps
Asset and project managers	Introduction, Overview, Key Concepts, Organising the organisation, Data Requirements, Implementation Guidance
Information and data managers	Introduction, Overview, Key Concepts, Data Requirements, Data Structure and Coordination, Data Management and Practice, Data, Implementation Guidance

Table 2: Reader's Guide

The diagram at Figure 1: IDMF Structure provides a layered representation of the structure of the document – the higher levels are more relevant to executive leaders, while those readers closer to the implementation of data requirements will require an appreciation of the full breadth of the framework.

A glossary of key terms and definitions is provided at Appendix B - Terminology.

2 Overview

2.1 Background

The NSW Government currently manages infrastructure assets worth more than $300 billion. Since 2013, the Government has invested more than $111 billion in building infrastructure to improve the lives of the people of NSW. In 2016-17, expenditure on asset management was $4.1 billion – a figure that is expected to increase due to the growth and age of assets. The NSW Government continues to invest significant resources across the asset lifecycle of state infrastructure, with an additional $93 billion of NSW government capital expenditure planned between 2019 and 2023, and with further expenditure committed beyond this timeframe.

Investing in and using technology and data to help optimise the management and operations of current and planned infrastructure assets will be critical. Infrastructure data has become an important part of state infrastructure management and operation. To achieve the greatest benefit the data must be managed as an asset in its own right.

Efficiencies and savings can be generated through enhanced management and sharing of infrastructure data:

- during strategic planning, planning and delivery of new projects
- across program portfolios
- in state-wide asset management including operations and maintenance.

2.2 State Infrastructure Strategy

The 2018 NSW State Infrastructure Strategy (SIS) proposed a series of recommendations to position NSW as an advanced user of smart Information and Communications Technology (ICT) to support state growth and digitally transform our approach to smart infrastructure.

Data on infrastructure can support better decision making across the infrastructure lifecycle. Smart ICT, such as sensors, provide information on the performance of infrastructure systems. As smart ICT is deployed across the State's infrastructure network, infrastructure-related data will become increasingly important in its own right. It will contain real-time performance information, including data on customer use. This rich information can be used to inform evidence-based, data-driven decisions, enhancing the efficient delivery, operation and maintenance of infrastructure for the people of NSW.

The State Infrastructure Strategy identified the IDMF as a key initiative to support coordinated, shared and trusted infrastructure data to better plan and operate the State's infrastructure systems. The Infrastructure Data Management Framework provides a framework for agency governance for the continuous collection, curation and sharing of infrastructure data, and provides guidance on consistent collection and central accessibility of information related to infrastructure risk and resilience.

2.3 Structure of the IDMF

The IDMF provides guidance to NSW Government and agencies on the application of better practices on infrastructure data management. The IDMF is structured around the following topic areas (see Figure 1):

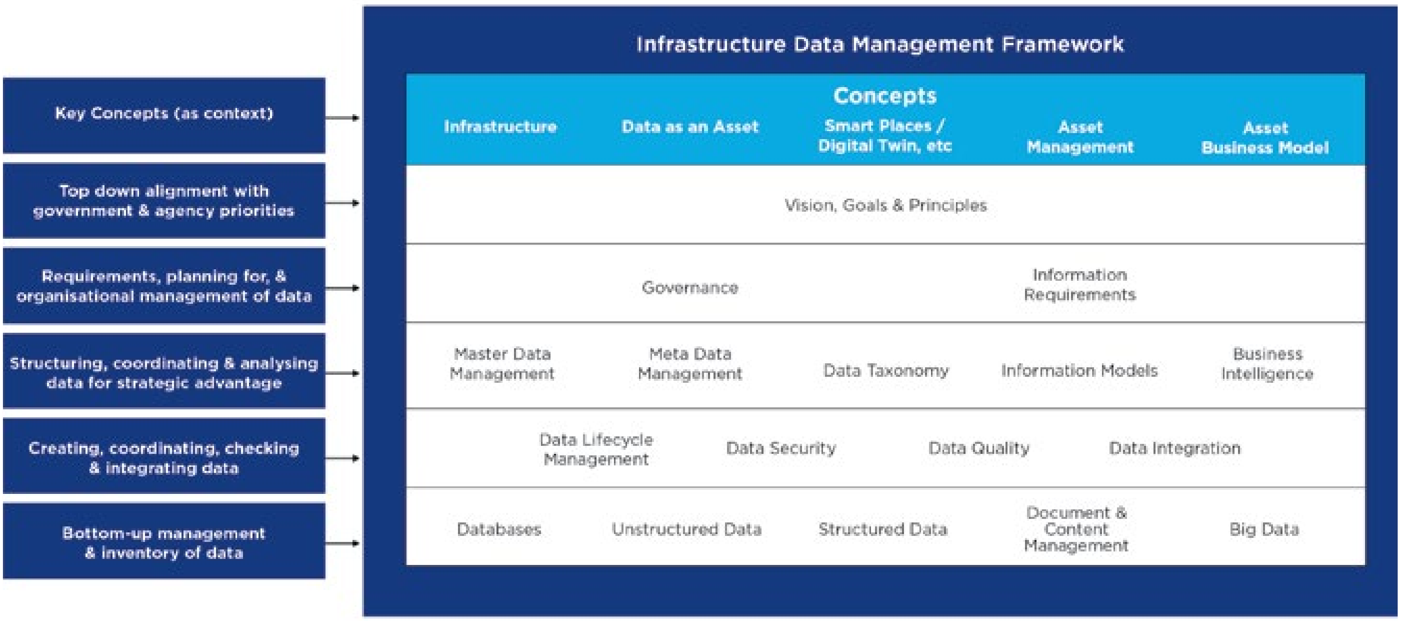

Key Concepts (as context)
Top down alignment with government & agency priorities
Requirements, planning for, & organisational management of data
Structuring, coordinating & analysing data for strategic advantage
Creating, coordinating, checking & integrating data
Bottom-up management & inventory of data
Infrastructure Data Management Framework
Concepts
Infrastructure
Data as an Asset
Smart Places / Digital Twin, etc
Asset Management
Asset Business Model
Vision, Goals & Principles
Governance
Information Requirements
Master Data Management
Meta Data Management
Data Taxonomy
Information Models
Business Intelligence
Data Lifecycle Management
Data Security
Data Quality
Data Integration
Databases
Unstructured Data
Structured Data
Document & Content Management
Big Data

Figure 1: IDMF Structure

The IDMF, as a key SIS initiative, comprises of:

- a principles-based approach to support consistent implementation of infrastructure data improvements across the state
- Common policies, frameworks, standards and other guiding information as foundation elements
- Identification of information requirements, which outline generic infrastructure related information requirements at an organisational level, and how that cascades down in the various phases of the asset lifecycle
- Identification of information models in response to information requirements, which are supported by data management requirements at each phase of the asset lifecycle
- Additional guidance and training materials providing more information on specific topics and training.

The NSW Information Management Framework (IMF) published in late 2018 outlines a shared direction for information management in the NSW Government. The IDMF extends the IMF to provide sufficiently detailed guidance to support the management of information and data relating to state infrastructure, which includes information and data related to assets such as utilities (e.g. energy and water), transport (e.g. land and water), communications, and the built environment. These elements work together to provide the data outcomes required from government owned and other state infrastructure.

2.4 Who is the IDMF for?

The primary audience is NSW Government agencies that own and manage infrastructure assets. Budget Material Agencies, State-Owned corporations, public financial corporations and local governments are encouraged to adopt relevant elements of the IDMF on new capital projects, including:

- Land acquisition and management
- Infrastructure
- Equipment
- Property developments
- Operational, communications and internet of things technologies that form components of a capital project.

The IDMF can also be applied to management of infrastructure data for existing assets.

Local governments will also find the IDMF useful, taking into consideration that some of the specific policies and obligations in the IDMF may not apply at the local government level. However, the majority of the content should still be relevant and applicable for local governments implementing infrastructure data initiatives.

2.5 How does the IDMF relate to other policies?

The IDMF is one of a suite of NSW policies, frameworks, standards and guidelines that have been developed to inform agencies on NSW Government requirements on information and data. Figure 2 shows the related information and data documents that should be read in conjunction with the IDMF.

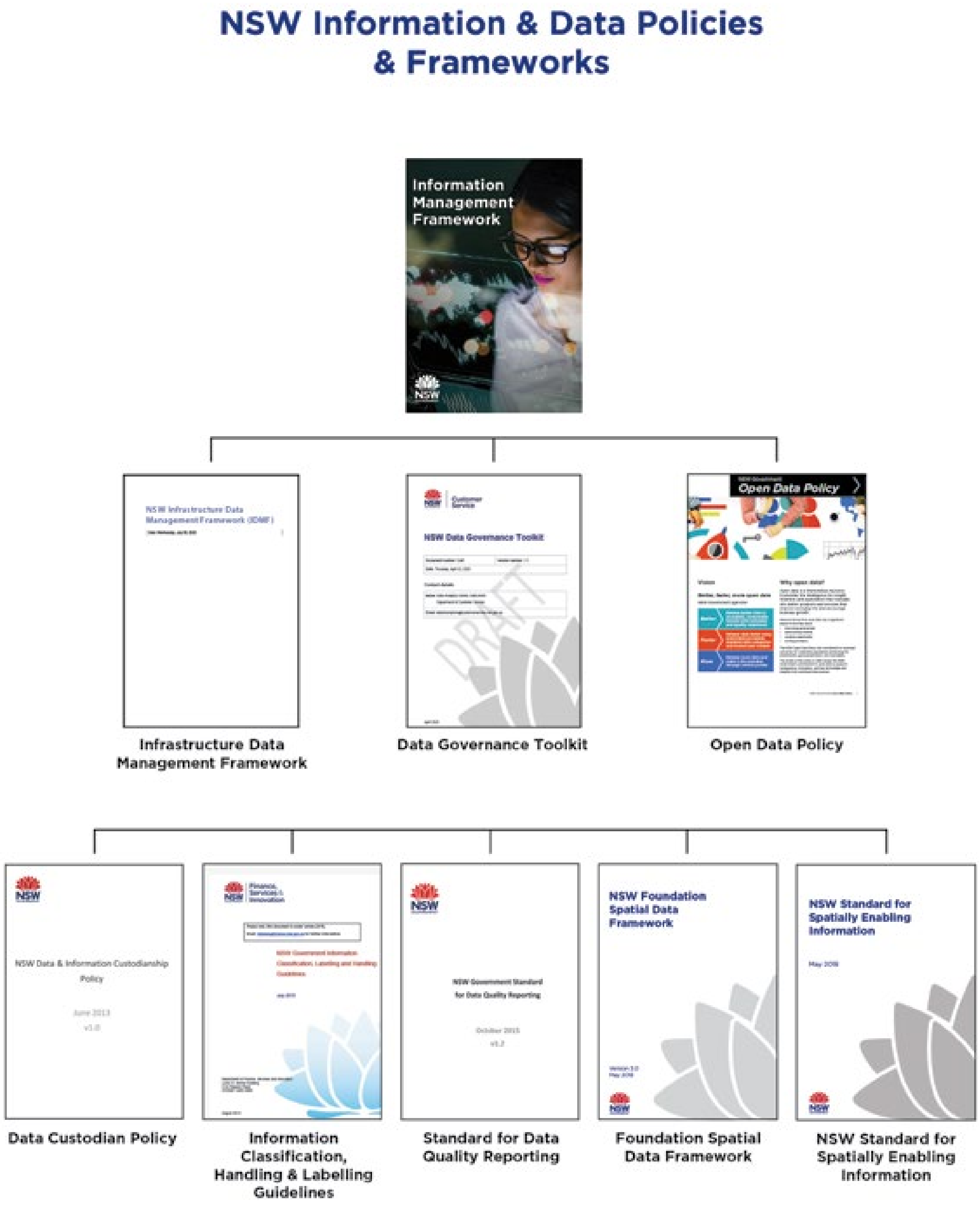

NSW Information & Data Policies & Frameworks
Information Management Framework
Infrastructure Data Management Framework
Data Governance Toolkit
Open Data Policy
Data Custodian Policy
Information Classification, Handling & Labelling Guidelines
Standard for Data Quality Reporting
Foundation Spatial Data Framework
NSW Standard for Spatially Enabling Information

Figure 2: Key NSW Data and Information Guidance

The IDMF also refers to other NSW Government policies, frameworks and tools that provide context and information relevant to infrastructure data in NSW, including:

NSW strategies

- AI Strategy
- Beyond Digital Strategy
- Smart Places Strategy
- State Infrastructure Strategy 2018-2038.

NSW Legislation

- *Data Sharing (Government Sector) Act 2015*
- *Government Information (Public Access) Act 2009*
- *Health Records and Information Privacy Act 2002*
- *Privacy and Personal Information Protection Act 1998*
- *State Records Act 1998*.

NSW policies

- Asset Management Policy
- Cyber Security Policy
- Internet of Things Policy
- Smart Infrastructure Policy.

NSW government frameworks

- Common Planning Assumptions
- Design System
- ICT Assurance Framework
- Information Management Framework
- Intellectual Property Management Framework
- Transport NSW Digital Engineering Framework.

National agreements

- Australian Building Information Modelling (BIM) Strategic Framework
- National Construction Code
- National Digital Engineering Policy Principles.

Other policies, strategies and frameworks that are not otherwise referenced may also be supported by the IDMF, for example in areas such as critical infrastructure protection, emergency management, climate change resilience, resource efficiency etc.

Note that while the IDMF provides guidance on the collection, curation and sharing of data, these are areas also subject to mandated legislative requirements. For example, both the GIPA Act and the *Privacy and Personal Information Protection Act 1998* create obligations for public sector agencies in relation to information management. The Framework is not intended to override existing agency policies and standards where they exist. Instead, it provides guidance and supplementary information for the development of agency policies and standards as they are developed or reviewed. It is important for project managers to contact their internal subject matter experts and teams for guidance on agency specific policies and standards and how these relate to the requirements of this Framework.

The development of the IDMF has also been informed by other frameworks, including from the International Organisation for Standardisation (ISO), from public and academic agencies in the United Kingdom, by the Victorian Digital Asset Strategy, as well as by innovative work in the digital engineering field conducted at agency level by Transport for NSW and NSW Health.

The IDMF will continue to evolve concurrently with developments in other jurisdictions, and NSW will continue to work closely with our national and international counterparts to ensure alignment with best practice. This includes alignment with national and international standards.

2.6 Maintaining the framework

Infrastructure data is rapidly evolving, and associated policies should be flexible and adaptable enough to accommodate changes. To ensure its usefulness, this Framework will be regularly updated as technologies change, opportunities and risks are better understood, associated and appropriate standards are developed, and as NSW Government's infrastructure data maturity grows. IDMF related components will be available from the Data.NSW IDMF website.

A working group/community of interest will be established to support users of the IDMF, and to manage changes in the framework over time, including development of new components. The IDMF will be formally reviewed on a regular basis.

The IDMF has been developed by the NSW Data Analytics Centre as part of the Department of Customer Service (DCS) portfolio of State Infrastructure Strategy projects. Further information is available at Appendix A – IDMF Project Background.

New Technologies Case Study: Data Sharing in Infrastructure

The UK National Infrastructure Committee commissioned a significant report from Deloitte in 2017 on New Technologies Case Study: Data Sharing in Infrastructure. A key gap identified by many stakeholders was the absence of an overarching set of principles that provided guidance and clarity on issues such as data ownership, what constitutes data, what might be interpreted as personal and non- personal, ensuring security by design, and so forth. While such a framework cannot ever be considered definitive, a common set of principles applicable across the whole sector (which can be customised) can be used as a starting point for subsequent data sharing, building on the work by industry groups to providing overall guidance.

The principles of the framework could cover areas including:

- Best practice guidance for organisations to carry out an internal audit of their data, classifying different types and identifying data that can be shared, either as open data or with restrictions.
- Best practice guidance for data quality and formatting for different categories of data.
- Approaches to specifying contracts that give appropriate emphasis to data requirements, clarity around responsibilities and liabilities related to data, and ensure there is scope for data to be used and re-used.
- Approaches to data anonymisation and aggregation so that confidential data may become shareable.
- Steps to deal with grey areas around data ownership, data and IP, personal and non-personal data, etc.
- Appropriate security measures for data sharing in infrastructure, building on the Government's '10 steps guidance' and NIS Directive principles to build awareness and understanding among infrastructure players, setting out explicitly how best practice in cybersecurity can be achieved by infrastructure organisations.

This framework would benefit from leadership by a public body with an invested interest in each industry, which would be complementary to the work carried out by industry-led groups. Inputs should be sought from industry and academia, and facilitated by public bodies such as regulators and NIC.

3 Key Concepts

The IDMF aims to provide support to a range of infrastructure concepts and principles by providing guidance to NSW Government policy makers, infrastructure owners, developers, maintainers and operators on the appropriate management of infrastructure data across the asset lifecycle, focusing on the data layer.

A key outcome in operating infrastructure is to define the information required to support decision making at the different levels in an organisation. A significant challenge associated with this objective is the ability for stakeholders to exchange the relevant data, information and knowledge from one stage of the lifecycle to the next in an open and structured manner. The infrastructure data collected must also support the ability to meaningfully aggregate the data, information and knowledge across different organisational levels.

Adopting the concepts and principles outlined in the IDMF will assist infrastructure stakeholders, including government and non-government partners, to:

- Identify appropriate information requirements across the asset lifecycle
- Agree appropriate data management activities for each stage of the asset lifecycle
- Define the information models to be created and managed for each stage of the asset lifecycle
- Agree the data exchange requirements, including timings, standards and formats the exchanges should comply with
- Agree on how the data collected about infrastructure assets satisfies the reporting and decision-making requirements at all organisational levels.

3.1 Standards

A standard is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.

A standard is a formalised method of achieving an interface between one entity, e.g. an organisation, and another. The process of applying a standard is repeatable, open and quite often transparent to the user, creating an information environment where the maximum amount of information is available to the maximum number of users.

The core process of this framework is based on the ISO 19650 *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling* suite of documents, in particular the relationships between information requirements and information models.

The NSW Asset Management Policy (TPP 19-07) was developed in line with the requirements of AS ISO 55000:2014 Asset management — Overview, principles and terminology, and agencies can use the requirements in AS ISO 55001:2014 Asset management — Management systems — Requirements to assist with the establishment, implementation, maintenance and improvement of their management system for assets. ISO 55001 also provides requirements on Asset Management Data that range from understanding the information needs to having processes in place for effective management of information.

Using common security standards and frameworks assists agencies managing their security risks. This includes risk and security management standards such as the AS ISO 31000 Risk management series of standards and the ISO/IEC 27000 Information technology - Security techniques - Information security management systems series. These can also help agencies align to the mandatory requirements of the NSW Cloud Policy, NSW Cyber Security Policy, NSW IoT Policy, etc.

Data standards – which include semantics, naming conventions, formats, and classifications – help to ensure there is a common understanding of the meaning of the data among stakeholders and that data can be exchanged, leveraged and reliably re-used by all parties interacting with the infrastructure.

It is best practice to adopt standards that are open, widely adopted and utilise global best practice, as opposed to custom or bespoke standards. This will ensure the data is transferrable across the asset lifecycle, as well as across different data platforms. This will also help support state-wide activities, such as the NSW Digital Twin, which relies on a range of standards including the NSW Standard for Spatially Enabling Information.

Standards will be identified and developed for use as part of the Infrastructure Data Management Framework over time, as agencies identify demand for further specific guidance. NSW Government is actively participating in the development of Australian and international standards, with the NSW Chief Data Scientist leading coordination of NSW Government input to smart places and data standards in collaboration with Standards Australia. A list of relevant international and Australian Standards is provided at Appendix C – Standards, and will be maintained on the IDMF website.

3.2 NSW Places and Infrastructure Initiatives

From an IDMF perspective, there are a number of NSW Government initiatives recommended by the State Infrastructure Strategy 2018-2038 that are changing the way that agencies should view spatial and infrastructure data, including:

- Smart Places
- Smart Infrastructure
- Digital Twin
- Digital Engineering
- Internet of Things
- NSW Open Data Portal (Data.NSW).

The primary relationships between these initiatives are illustrated in Figure 3, which highlights the importance of establishing the foundation data layer, including achieving optimal alignment with the higher level initiatives. It holds implications and benefits for all layers of the smart information pyramid as these initiatives will greatly benefit from the adoption of a consistent approach to information and data management.

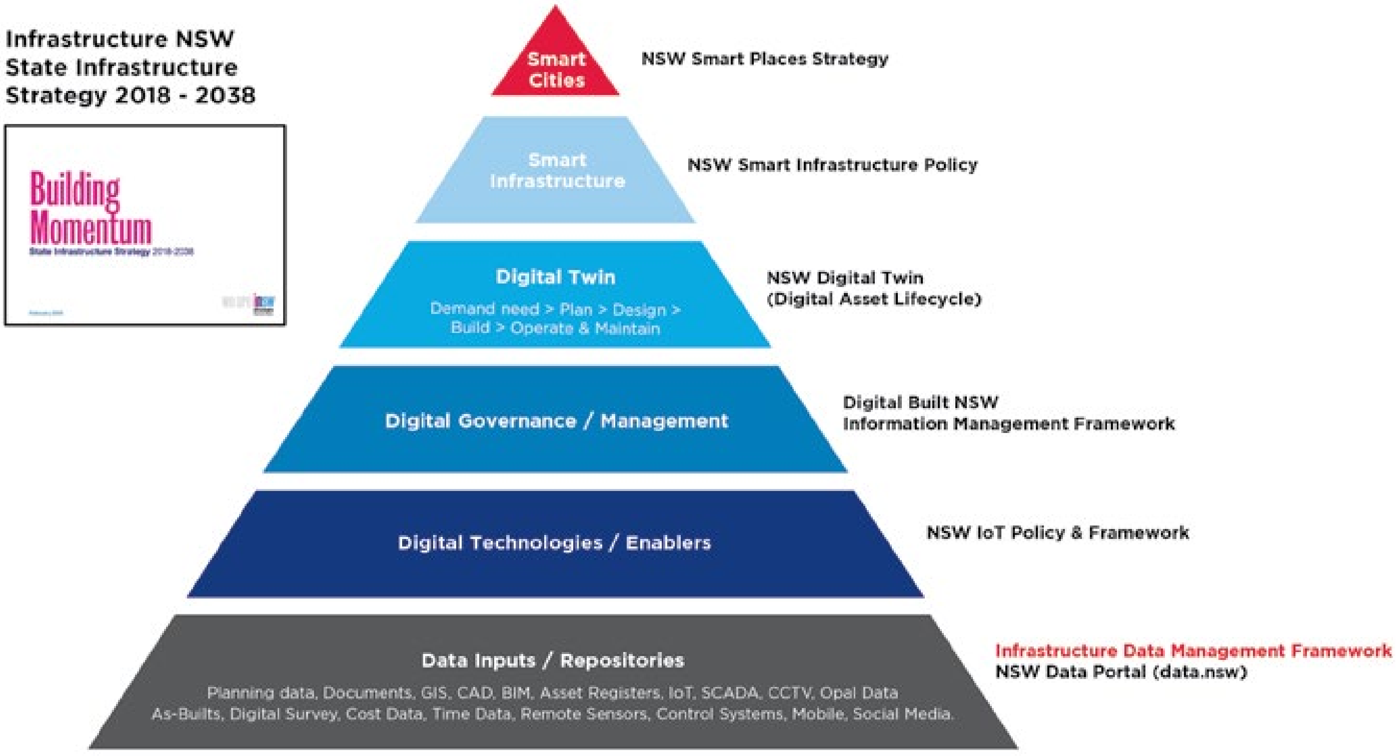

Infrastructure NSW
State Infrastructure
Strategy 2018 - 2038
Building Momentum
State Infrastructure Strategy 2018-2038
Smart Cities
NSW Smart Places Strategy
Smart Infrastructure
NSW Smart Infrastructure Policy
Digital Twin
Demand need > Plan > Design > Build > Operate & Maintain
NSW Digital Twin
(Digital Asset Lifecycle)
Digital Governance / Management
Digital Built NSW
Information Management Framework
Digital Technologies / Enablers
NSW IoT Policy & Framework
Data Inputs / Repositories
Planning data, Documents, GIS, CAD, BIM, Asset Registers, IoT, SCADA, CCTV, Opal Data
As-Builts, Digital Survey, Cost Data, Time Data, Remote Sensors, Control Systems, Mobile, Social Media.
Infrastructure Data Management Framework
NSW Data Portal (data.nsw)

Figure 3: NSW Infrastructure Smart and Digital Initiatives

3.2.1 Smart Places and Smart Infrastructure

The NSW Smart Places Strategy provides a vision of the use of technology to collect and use spatially enabled data to make better, evidence-based decisions to improve the productivity, liveability and resilience of cities, towns and communities.

The Smart Places Strategy details an action plan with three focus areas.

- Foundations - Standards and policies to enable consistent implementation and benefits realisation
- Enablers - partnership and procurement improvements
- Programs - new and renewed place transformation and initiatives to drive digital inclusion.

The Smart Places Strategy also outlines the NSW Government's commitment to providing smart infrastructure that produces, analyses and helps to securely share data, using the best available technologies to capture project, operations and service data.

To assist agencies to embed smart technologies in future infrastructure, the NSW Government has developed the NSW Smart Infrastructure Policy to make sure agencies plan, design, build and operate connected communities, and use infrastructure assets to their full potential. Smart infrastructure will help to realise benefits including improved customer outcomes, productivity improvements, information driven decision making and whole-of-lifecycle asset management.

3.2.2 Digital Twin

A Digital Twin is a digital model of a real-life object, process or system. The digital model can be informed by historical data and fed with live sensor data to make the digital model a 'twin' of the real-life, real time subject. Digital Twins of discrete systems can be linked to create twins of larger, more complex systems such as a factory or a city. Figure 4 provides a visual representation of the disparate data layers that can be integrated to provide real time, spatially enabled insights leading to better decisions and better outcomes.

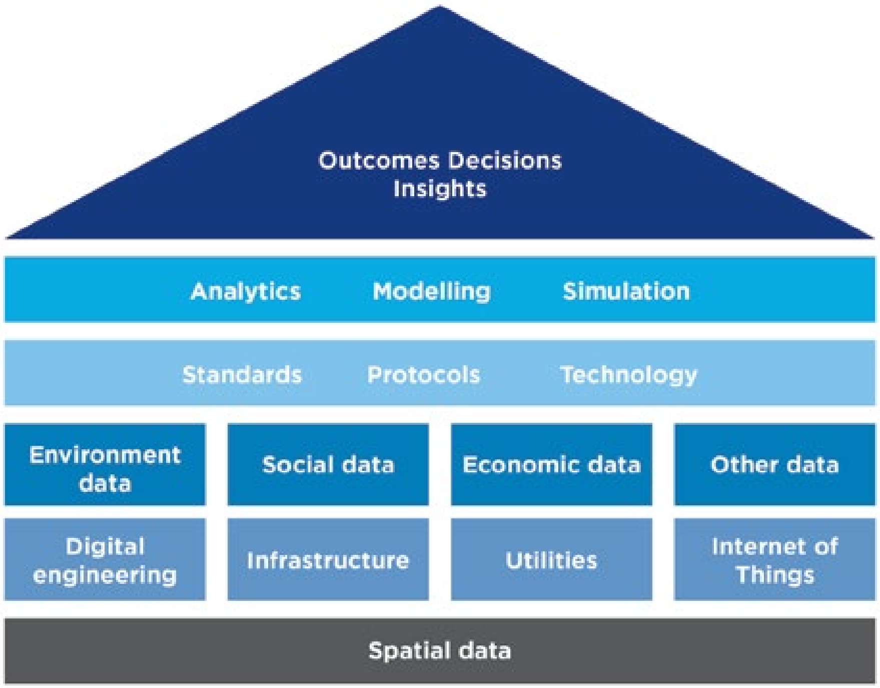


Figure 4: Integration of multiple data types and sources in spatially enabled digital twins

Adapted from the ANZLIC Principles for Spatially Enabled Digital Twins of the Built and Natural Environment in Australia

The NSW Digital Twin is an interactive platform to capture and display real-time 3D and 4D spatial data in order to model the built environment. This is a step change from storing and visualising spatial data in 2D. The NSW 'Digital Twin' will help facilitate better planning, design and modelling for future needs. The platform also integrates digital engineering assets, building information models, and live API feeds for public transport, air quality, and energy production. The platform is also designed to integrate with the NSW Spatial Collaboration Portal that provides a central point to search, discover and share spatial information.

The NSW Spatial Collaboration Portal provides a platform for publication and access controlled use of spatially enabled data, and a repository for data to be made available to the Digital Twin viewer. The list of standard data formats that may be used on the Portal are listed at Appendix C – Standards.

3.2.3 Digital Engineering

The National Digital Engineering Policy Principles define Digital Engineering as: the convergence of emerging technologies such as Building Information Modelling (BIM), Geographic Information Systems (GIS) and related systems to derive better business, project and asset management outcomes. Digital Engineering enables a collaborative way of working using digital processes to enable more productive methods of planning, designing, constructing, operating and maintaining assets through their lifecycle.

Digital Engineering activities and systems must also merge with existing asset management practices and integrate with existing Asset Management Systems. The level of maturity of the existing environments must be taken into consideration when developing a 'fit for purpose' enterprise wide system (ecosystem) able to support a range of agencies and their assets.

An action from the NSW Smart Places Strategy is the development of a Digital Built NSW approach with the aim to develop a digital engineering policy, framework and roadmap for NSW. Together with the Asset Management Policy, Digital Built NSW will enable a thriving NSW digital economy for the built environment, encouraging growth and competitiveness and facilitating a more effective use of current and future infrastructure assets.

3.3 Data as an Asset

Data and information are critical assets that drive accountability, enable deep insights and inform decisions. Key challenges to realising value of insights and decisions are governing, harnessing, managing, protecting, using and reusing the vast amount of information and data generated by transactions systems, administrative systems, operations systems and sensor networks.

NSW Government is recognising the value of data, including incorporating it as one of the key principles in the Information Management Framework, e.g. that data is:

*"**Secure, valued and managed as an asset** - Information is recognised as a core component of government services and operations, supported and maintained as a secure, long-term business asset wherever required"*

Through the recommendations of the State Infrastructure Strategy there is now a more defined approach to how technology can be used to get more out of existing and new infrastructure assets. The combination of existing data and new technologies that can be used to analyse data at a deeper level will be key to getting more out of existing infrastructure. This includes areas like sensors, digitalisation, the Internet of Things (IoT), big data, and Artificial Intelligence (AI), which will lead to improving how NSW Government collectively manages and operates infrastructure, maintains existing assets, and enhances the capacity and resilience of infrastructure networks. At a fundamental asset management level, data must be treated as vital and agencies must have a fit-for-purpose asset register able to support lifecycle costing capability to enable decision making across the asset lifecycle.

In NSW Government, information management is a key component of the digital transformation of government. Both the Information Management Framework and the SIS identify that information is a valuable asset to be managed and provides a practical approach to help agencies govern, harness, manage, protect, use and reuse information and data in their digital transformation initiatives.

Implementing the SIS recommendations, including the IDMF, will improve the level of information and data alignment and integration, however this needs to be done in a coordinated and collaborative way.

3.4 Infrastructure Data as an asset

For the IDMF, infrastructure is defined as:

"The basic economic and social services, facilities and installations to support society including water, wastewater, transport, sport and culture, power, communications, digital and data, police and justice, health, education and family and community services."

Note: Based on INSW's Infrastructure Investor Assurance Framework (IIAF) http://www.infrastructure.nsw.gov.au/media/1269/final-pub-iiaf-paper-v-522_web.pdf; further definitions are at Appendix A.

Well-developed and maintained infrastructure supports increased productivity and allows for increased economic possibilities to support general sustainable development and economic growth. The presence of well-developed and well-maintained infrastructure also enables people and businesses to invest in sectors that are more infrastructure usage based.

Infrastructure data can be categorised as information and data that may be collected and managed to improve and coordinate infrastructure planning, development, delivery and operation. These activities occur between key stakeholders, both inside and outside government.

The National Infrastructure Data Collection and Dissemination Plan (NIDCDP) (Jun 2018) defined six broad categories that should be taken into consideration in developing infrastructure data and information requirements. The categories are:

1. Infrastructure stocktake – identify the owner, type and location, etc. of assets
2. Infrastructure performance – identifying and understanding the performance of assets
3. Infrastructure investment and planning – information on infrastructure to promote planning, decision making, and investment
4. Impact of infrastructure – quantify, understand and better assess the economic, environmental, social and safety impacts of assets
5. Infrastructure use (Transport, Energy, Water and Communications) – information required to improve planning, management and policy development
6. Data and information for decision and innovation – identifying how to improve the availability, discoverability and accessibility of government and non-government infrastructure data and information.

Plain language (enduring) questions are available for each of these categories in the NIDCDP.

The UK's National Infrastructure Commission report, Data for the public good adopted the approach that the more information available on infrastructure, the better it can be understood, and concluded that data is crucial to the management of infrastructure. In line with their findings and proposed approach, the NSW State Infrastructure Strategy requires data to be treated as infrastructure.

Data improves how infrastructure is planned, designed, built, managed and decommissioned, with real-time data informing how infrastructure is used and operated. However, collecting data alone will not improve the infrastructure. The key goal is to collect high-quality data and use it effectively to support improved decision making.

NSW Government is investing in new and existing infrastructure, which is improving the lives of the community and citizens. Continued realisation of the benefits provided by the new and improved infrastructure requires an improvement in the quality of the infrastructure data, and a shift towards improved collaboration between government, industry and citizens. This can be achieved through a shift towards embracing structured and standardised data that can be shared to improve decision making.

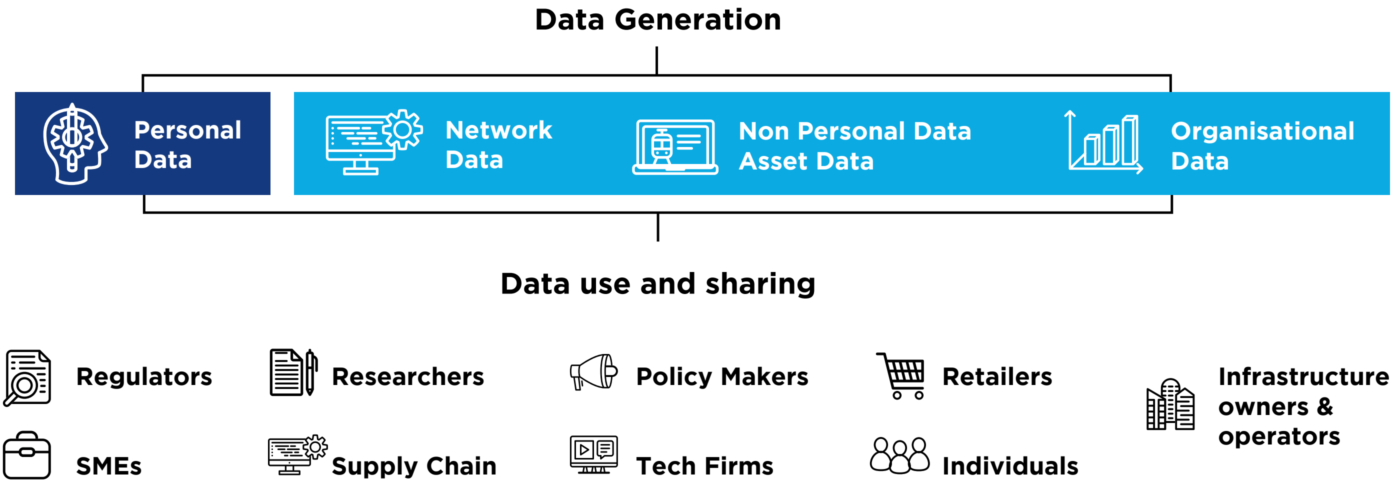


Figure 5: Data is generated across the infrastructure sectors and used by a variety of stakeholders

Source: https://www.nic.org.uk/wp-content/uploads/Data-sharing-in-infrastructure.pdf

Infrastructure Data also needs to be considered within the context of the asset management lifecycle. Data security and the ability to share data varies across the different stages of the asset lifecycle and data needs to be updated, stored securely, and preserved for future use, which for infrastructure assets can be up to 100 years or more. Data must also be supported by physical infrastructure such as sensors, high speed connectivity, data centres, etc.

3.5 Asset Management

Asset management can be defined as the coordinated activity of an organisation to realise value from assets, present and future. Value can represent financial return and/or be measured by the contribution the assets make to service delivery through both function and performance.

The NSW Asset Management Policy sets out core asset management practices for NSW Government agencies to adopt and also mandates a whole-of-government and whole-of-asset-lifecycle approach.

A core element of effective asset management is having decision-making that is evidence-based and data-driven. A pre-requisite for this to happen is to collect sufficient data, and ensure accuracy of the data and documentation in order to:

- Support development of assets
- Support efficient operation and maintenance of assets
- Support effective communication with all stakeholders, from whole-of-government decision makers to the public as users of the infrastructure
- Meet legal and statutory requirements
- Ensure the smooth transition of the asset from one stage in its lifecycle to the next.
- Monitor Asset Financial Management
- Monitor Asset Condition/Performance
- Monitor the Asset Audit and Assurance.

As defined by the State Infrastructure Strategy's six strategic directions, the NSW Government is constantly striving to improve the decisions made around infrastructure, whether it involves:

- Strategic assessments
- Planning and development
- Project approvals
- Maintenance and operation of existing and new infrastructure assets, or
- Replacement or disposal of assets outside of their useful life.

NSW Asset Management Policy for the NSW Public Sector

The Asset Management Policy for the NSW Public Sector (TPP 19-07) provides guidance and requirements on decision making during the operations and maintenance phases of government owned assets. Agencies also have their own agency level policies and procedures to assist with improving decision making on infrastructure across the asset lifecycle.

The policy defines the asset lifecycle as all the stages an asset experiences over the period from conception to end-of-life or contract, including planning, acquisition, delivery, operations and disposal. Depending on the type of project and asset, the responsibilities of an asset owner, asset manager and operator may change across the lifecycle.

The IDMF plays a key role in supporting decision making by ensuring that agencies can identify data requirements, and that data on infrastructure is collected and used to better support data driven decision making. Several frameworks exist to support agencies to make better decisions during the different development and delivery phases, including:

- Infrastructure Investment Assurance Framework (IIAF)
- ICT Assurance Framework
- Infrastructure Australia's Assessment Framework (for Federally funded programs).

The generic infrastructure asset lifecycle shown below illustrates the typical lifecycle stages as defined in ISO 55000:2014 Asset management - Overview, principles and terminology and by the Institute of Asset Management (IAM), and is used in the IDMF to support concepts and requirements defined within the framework.

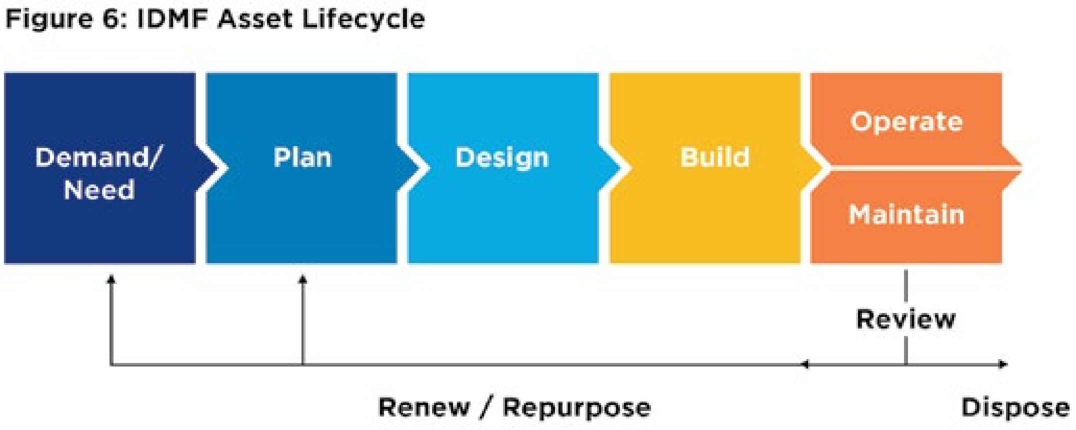


Figure 6: IDMF Asset Lifecycle

The asset lifecycle consists of the following stages:

- **Demand / Need** – This initial stage establishes and verifies operational, service and associated infrastructure asset requirements. For existing infrastructure, it is based on the performance of the existing assets and their potential to meet service delivery needs, while for new assets it is determined based on the requirements for new infrastructure to meet service delivery requirements.
- **Plan** – Based on the requirements developed in the Demand / Need stage the project will select the best concept (options) for Design and Build stages. Following the necessary approvals, the proposed solution is progressed through the specification and procurement processes.
- **Design** – Design is focused on enhancing the design of the preferred option, ensuring that it is fit-for-purpose and able to meet the customer’s requirements.
- **Build** – Following approval of the final design the infrastructure assets are constructed in accordance with the approved design and handed over to the Operator / Maintainer.
- **Operate and Maintain** – During the Operate and Maintain stage the infrastructure assets are placed into service and maintained with the aim to optimise the condition of the assets whilst supporting the functional performance of the assets to deliver the required services.
- **Renew / Repurpose** – When an asset reaches the end of its useful life or is not able to support the service delivery requirements, the functionality, performance and cost of the asset are reviewed, and if feasible, recommended for renewal or re-purposing.
- **Dispose** - When an asset reaches the end of its useful life and is not suitable for renewal or repurposing the asset is the disposed of in the appropriate manner.

3.5.1 Agency Asset Operating Model

NSW Government agencies use various models for the outsourcing of planning, design, construction and operations and maintenance of infrastructure assets. The level of outsourcing may be determined by the entity’s overarching operating model or defined by the management requirements of an individual service and its associated infrastructure assets, including the need to access specialised expertise that may not be held within government.

A generic operating model (adapted from the TfNSW Asset Business Model (2020)) has been adopted by the IDMF to illustrate the types of roles and associated responsibilities fulfilled by various government and industry stakeholders. The important interactions demonstrated by this Asset Operating Model are the exchanges of asset related data and information between the various stakeholders at different stages of the asset lifecycle.

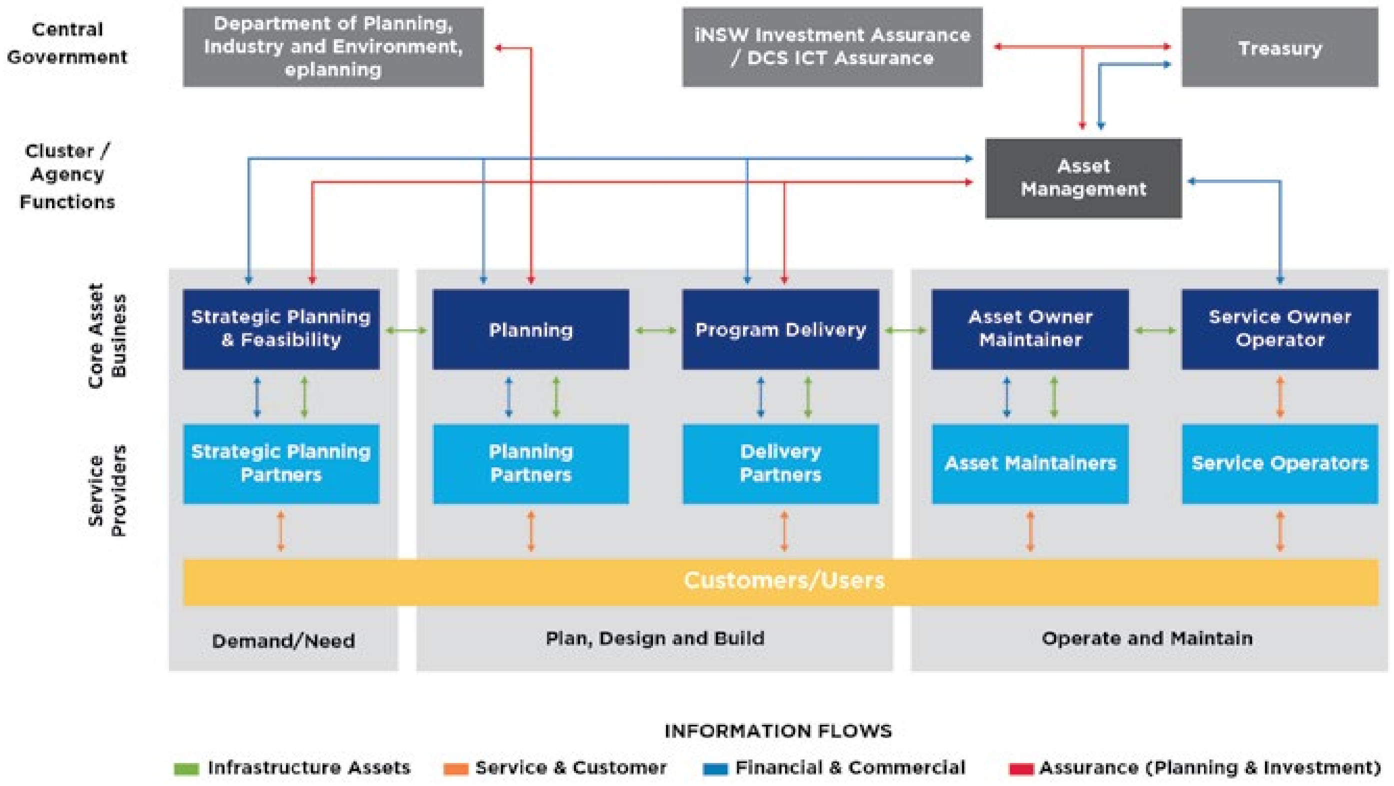


Figure 7: Agency Asset Operating Model

It is critical to the overall success of infrastructure data use that the specific information and data requirements are coordinated across the asset lifecycle, and also clearly specified in contracts with delivery partners. The specification of data requirements should be completed as a collaboration between functional units responsible for infrastructure, data and assurance.

NSW Government agencies use various models for the outsourcing of planning, design, construction and operations and maintenance of infrastructure assets. The level of outsourcing may be determined by the entity's overarching operating model or defined by the management requirements of an individual service and its associated infrastructure assets. Section 121 of the GIPA Act ensures that where an agency outsources its service delivery functions there is an immediate right of access to relevant information contained in records held by the contractor. Agencies should be aware of the relevant obligations under this provision, as well as the contract disclosure requirements under Part 3 Division 5 of the GIPA Act.

The operating model also highlights the need for coordination and collaboration between agencies to provide consistent and comprehensive information to central government stakeholders, including INSW, Treasury and Cabinet, to support government portfolio level decision making.

3.6 Application of the IDMF

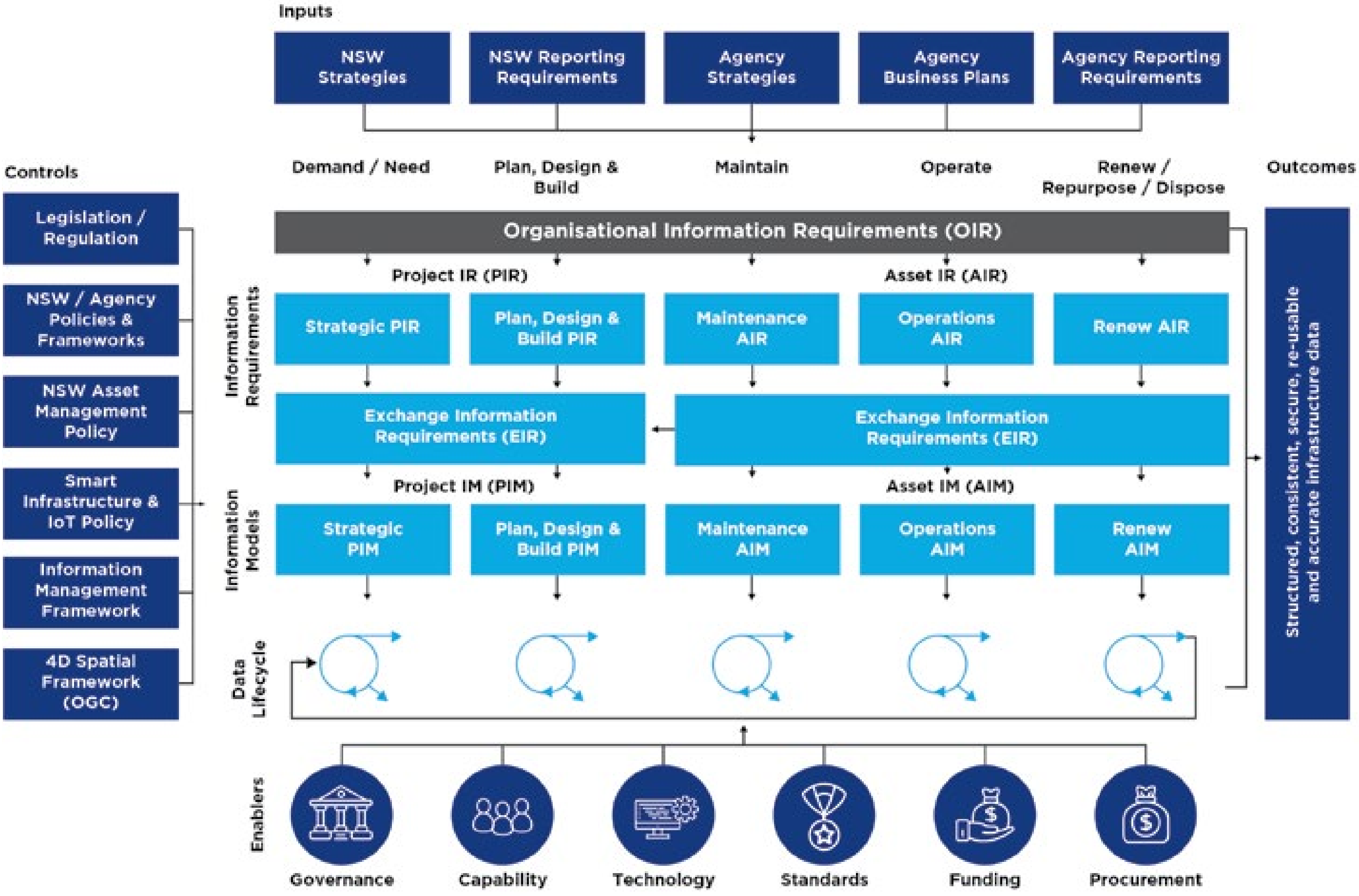


Figure 8: IDMF Context: Inputs, Controls, Process and Enablers

As illustrated in the IDMF context diagram in Figure 8, the framework consists of four key elements. State-wide adoption of a unified approach to infrastructure data management requires the alignment of these different concepts to ensure optimum benefits are achieved from infrastructure data:

- **Inputs**, which essentially are all the contextual strategies, business plans and reporting requirements that govern and inform NSW agency operations and which need to be considered when developing organisational information requirements;
- **Controls**, which include all legislation, regulation and other NSW Government frameworks that define how infrastructure assets, projects and associated data should be managed within NSW Government agencies;
- **Process**, which builds upon Australian and international standards to illustrate the iterative application of a managed data lifecycle over the lifecycle of infrastructure from identification of a demand or need for new investment, through the planning and acquisition process (including construction), to asset maintenance, delivery of services and the eventual decision to dispose of or recycle the infrastructure.
- **Enablers**, which include the enterprise elements required to properly support the IDMF. The use of identified standards will allow consistency, regardless of variation of organisational structures, maturity, technology and procurement practice.

4 Organising the Organisation

4.1 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 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 how their work contributes to organisational objectives and outcomes. Agencies with good data governance practices are better able to understand and manage risks for their data, while extracting the maximum value from them.

When an agency implements the IDMF, it is important to establish robust data governance as a key agency process and responsibility. This includes identification of key executive sponsors, skills and capabilities, allocation of responsibilities and authorities and establishment of organisational processes and procedures.

The NSW Data Governance Toolkit is a valuable resource designed to assist NSW Government agencies to develop their own data governance capability, and it can be applied to the development of data governance arrangements in an infrastructure data program context.

The Toolkit outlines a Data Governance Model that specifies data governance activities across four tiers:

- Strategy and Planning – agencies should define the program's values, vision and mission.
- Organisational Structures, Roles and Responsibilities – agencies need to ensure accountability and decision-making authority for data-related activities are appropriately assigned and formalised.
- Organisational Enablers – agencies need to ensure there is a strong motivation to achieve good governance within an organisation as well as the requisite capabilities, in terms of people and technologies.
- Data Management – agencies need to ensure their data governance program comprises the core data management functions, such as data quality, data security, metadata etc, as outlined in the Data Management Body of Knowledge (DAMA-DMBOK).

NSW Data Governance Toolkit

The NSW Data Governance Toolkit provides agencies with 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 as 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.

https://data.nsw.gov.au/data-governance-toolkit-0

4.2 Technologies

With the increasing speed, volume and complexity of data in modern society, humans are becoming more reliant than ever on technology to manage and monitor data. The capture, management and use of infrastructure data is supported by a range of technologies, such as design, project management and building information modelling software, which are widely used within the construction sector. However, interoperability and collaboration are important considerations in the use of these technologies.

A key consideration in adopting various technologies includes the decision on the most appropriate technology architecture. The vision to establish digital twins to enable smart places and infrastructure will require the establishment of digital twins at different levels within NSW Government. This increases the importance of an ecosystem of connected technology environments (platforms) to enable all the stakeholders to connect their systems at the data layer, as illustrated in Figure 9.

Figure 9: Inter-Connected Data Environments

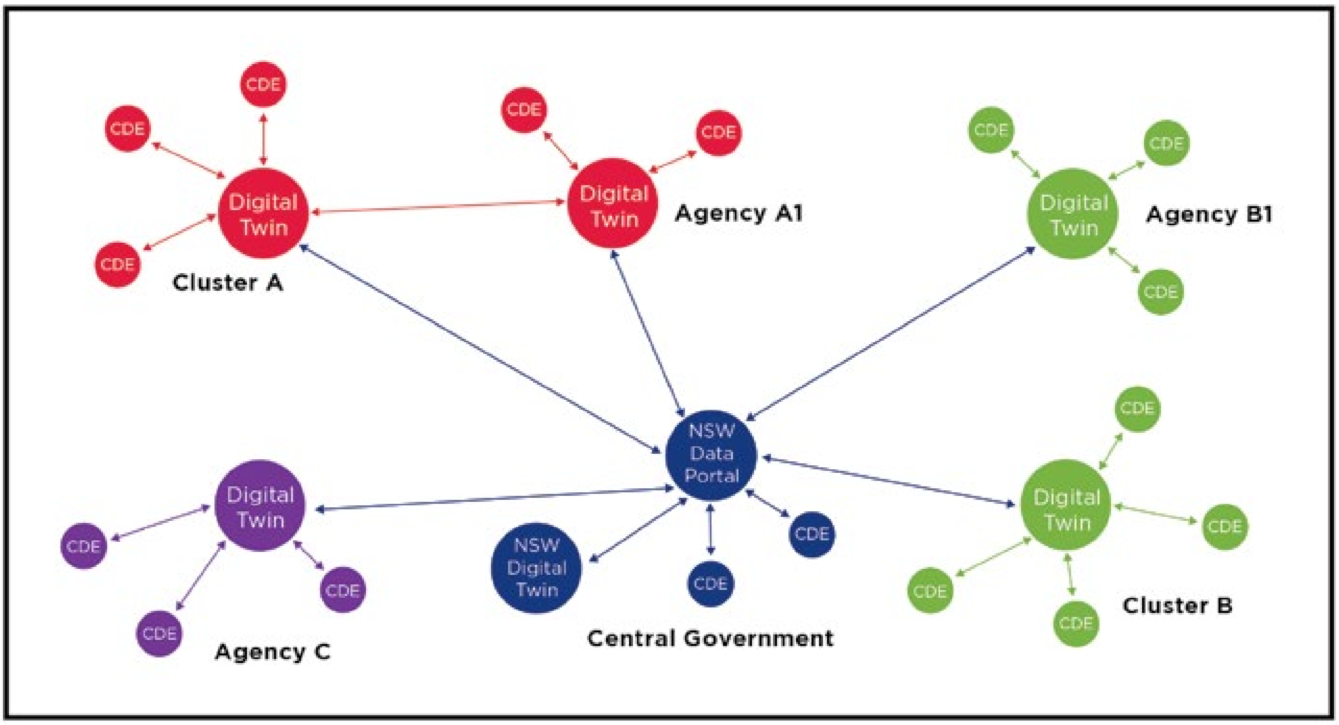


Figure 9: Inter-connected data environments

NSW Government is on the way to successfully connecting the different environments of agencies through Data.NSW and the NSW Digital Twin, however it requires technology platforms to become more "open" for all stakeholders to participate in a connected data ecosystem.

From an infrastructure data perspective, the ability of software platforms to support the relevant open data standards will become more important over time. If this state of inter-connected ecosystem is not achieved NSW Government and agencies will continue to need to support complex data transformations between different technology platforms.

What good looks like

- Interoperable: Systems are set up to facilitate operating effectively in inter-connected data environments (for more detail, see Section 4.2.1 on Common Data Environments)
- Secure data access for multiple project parties
- Faster, consistent setup for new projects
- Offsite access to drawings and project information
- Faster, more informed approval
- Less admin and more efficient data processing
- Enterprise technologies for the data analysis of business information
- Graphical user interfaces to provide summarised report views of data
- Processing of large volumes of data
- Capture of large volumes of spatially enabled real time data
- Permission based access to sensitive data.

How to achieve good practice

- Invest in data storage and exchange in common environments
- Ensure IT platforms are pre-configured to enable infrastructure data management
- Infrastructure data is accessible on mobile platforms
- Procure or develop software for reviewing 3D/BIM models
- Develop bulk production drawings from 3D/BIM models
- Invest in Business Intelligence and Data Analytics
- Utilise dashboards to provide accessible and interactive views of data
- Develop Artificial Intelligence / Machine Learning capabilities to improve data processing efficiencies
- Invest in Internet of Things (IoT) to enable capture of spatial data
- Utilise data sharing platforms that enable permission-based access to sensitive data.
- Require consistent application of modern Coordinate Reference System(s) and spatial data transformation(s).

At an Agency level it is important to define how to establish interconnected environments for different phases of the asset lifecycle, including how best to share and connect information between the agency and industry partners. This ability to share and connect is created through the establishment of Common Data Environments. To ensure consistency the use of Industry Reference data environment models and domain-specific models should be adopted where possible.

4.2.1 Common Data Environments

A Common Data Environment (CDE) is defined in AS ISO 19650.1:2019 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) - Information management using building information modelling, Part 1: Concepts and principles as the agreed source of information for any given project or asset, for collecting, managing and disseminating data and information through a managed process.

A CDE is essentially a collective name given to a group of integrated IT systems within an organisation that enables users to store, collaborate and exchange information and data. A CDE could be a project server, extranet or file-based retrieval system. Increasingly CDEs use cloud-based software to hold and share the relevant infrastructure information.

Agencies typically will have a CDE for the receipt, validation and approval of information delivered by suppliers, while suppliers will have a supply-side CDE used by their teams, including sub-contractors, which is illustrated in Figure 10. The relationships between the CDEs are shown in parallel with the Asset Operating Model in the top half of the figure to represent the changing CDEs over the lifecycle of the asset.

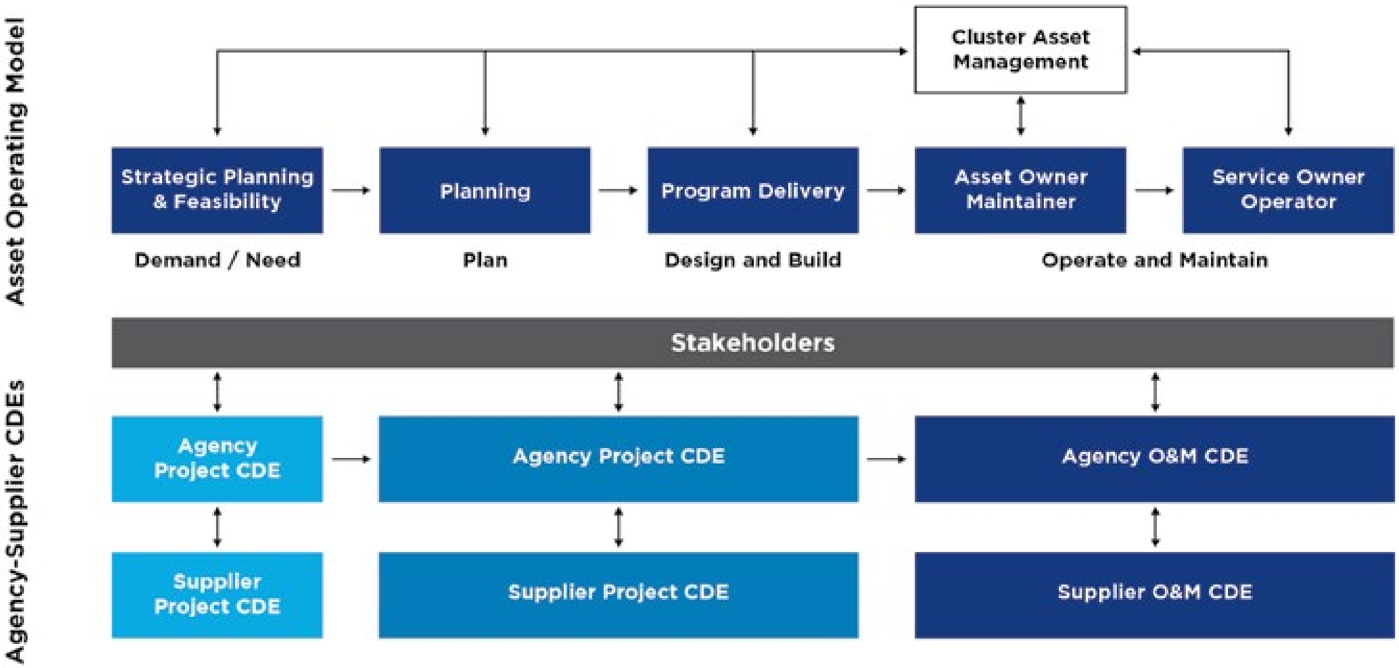


Figure 10: Agency-Supplier CDE interfaces

Even though the term CDE is primarily used in the context of projects, the concept applies to all phases of the asset lifecycle, where an enterprise asset management system would be the primary component of a CDE during the Operations and Maintenance (O&M) phase.

Benefits of using a CDE

The CDE as the single source of information means there is no uncertainty about which version of information should be used or referenced. The CDE should serve as the ultimate source of 'truth' and bring a number of benefits for all stakeholders:

- Shared information should result in coordinated data which will, in turn, improve efficient and effective activities and decisions
- Reduce the time and effort required to check, version and reissue information
- Reuse of information to support construction planning, estimating, cost planning, facilities management, and other O&M activities
- Reduce the time and cost of producing coordinated information
- Improve spatial co-ordination through use of a centralised 3D model (BIM and/or GIS)
- Production of models, documents and data should be right first time assuming that contributors follow agreed processes for information development and sharing
- Improve spatial co-ordination through use of agreed Coordinate Reference System(s) and spatial data transformation(s).

CDE requirements

The successful management of information in a CDE requires agreement from key stakeholders on:

- information formats
- delivery formats
- structure of information models
- the means of structuring and classifying information
- attribute names for metadata, for example documentation numbering schemas, and asset and location classifications.

The development of smart places and smart infrastructure (including the use of smart sensors) will significantly increase the volume of data that will be managed and shared. The large volumes of data involved will require the use of dedicated data management and analytics technologies.

One of the key challenges for infrastructure data management is making use of the vast amounts of data now being collected. Advanced Analytics, Artificial Intelligence, and other forms of machine learning can help to extract maximum information (value) from the huge volumes of data about infrastructure assets. Machine learning tools can enhance data integrity by eliminating human error, free up resource hours and significantly cut costs. More information on suitable technologies are provided in the Internet of Things Policy and Smart Infrastructure Policy.

It is recommended that agencies include these requirements as part of maintaining their infrastructure technology environment. There is a global shift to cloud-based solutions to support data storage and exchange, which needs to be managed in accordance with relevant cyber security requirements. Agencies must ensure they comply with NSW (and Federal) cloud policies, in particular requirements on the classification and secure storage of data, especially if data centres or servers are not in Australia.

4.3 Procurement

Procurement plays a central role in the successful delivery of infrastructure projects, and it is critical to clearly address data requirements in contracts with service providers. Contracts need to address the matters outlined in this section as well as any other relevant policies, including the Cloud Policy and the Smart Infrastructure Policy.

What good looks like

- Clarity on data governance for infrastructure projects – particularly data sharing arrangements;
- Faster, more consistent tender preparation;
- Less complexity and improved tender responses (more due diligence);
- Informed tender assessment; and
- Smooth project start-up.

How to achieve good practice

- Develop an agreed commercial and legal framework for infrastructure data, including clearly identifying data ownership and associated rights;
- Develop a data sharing agreement that outlines roles and responsibilities for securely managing data;
- Develop a standardised approach with template documents;
- Establish scalable, integrated procurement processes fully integrated with existing NSW Government assurance frameworks;
- Utilise guidance and technical support for infrastructure data procurement; and
- Utilise expertise to support project initiation.

4.3.1 Data handling

Infrastructure systems often need multiple service providers to provide hardware, software, and connectivity. Health checks should be conducted at key stages of the lifecycle. Agencies need to require service providers to perform due diligence and identify all parties involved in developing and delivering these products and services. This due diligence includes following applicable NSW Government policies including the Asset Management Policy (TPP 19-07). The applicable policies and frameworks may vary for each project and so it is important to identify the required assurance processes such as the Infrastructure Investor Assurance Framework (IIAF) and ICT Assurance Framework.

The majority of infrastructure data that agencies manage relates to management of existing infrastructure assets. This data will not be required for investment decision making, but to support how best to maintain the existing agency asset portfolio. Service providers must be transparent about their data handling and storage practices so that there is full visibility of all parties who have access to the data generated by service providers across all phases of the asset lifecycle.

4.3.2 Data ownership and rights

This section should be considered in conjunction with Section 7.4 for data privacy and security as restrictions on the usage of data are intertwined with ownership.

4.3.2.1 Data ownership and control

Agencies should determine whether data is owned by a vendor, and if so, in what circumstances when developing an infrastructure system. This determination should include an assessment of the sensitivity of the data. For projects where a vendor owns data, agencies should ensure their contract enables them to have reasonable control over government data contributed as part of a project. Agencies should define data governance requirements in contractual approaches and stipulate their requirements for what data is being collected, where it is stored, who can access it, at what granularity and for what purpose.

In circumstances where the service provider owns the data, agencies should identify whether they are entitled to sell the data contributed by them to a third party, and understand any contractual rights to see, use and monetise this data. If this use is unacceptable, agencies should look for other service providers who have data policies that allocate ownership, use and reuse rights to the purchaser. Refer to NSW Crown Copyright policy for more information.

Organisations that provide infrastructure often have direct legal responsibilities to customers or users affected by the operation of the infrastructure, even if the use of the infrastructure is by other entities (such as third-party service providers). The rights and responsibilities of each entity within a data ecosystem need to be clearly stipulated in the contract. Contracts should specify who the data controller is and create appropriate restrictions, controls and safeguards as to the roles and responsibilities of the other entities. Information access rights in relation to infrastructure data assets, especially where government agencies are contracting with third party service providers, are covered by section 121 of the GIPA Act and agencies are reminded to consider this provision when entering into outsourcing arrangements.

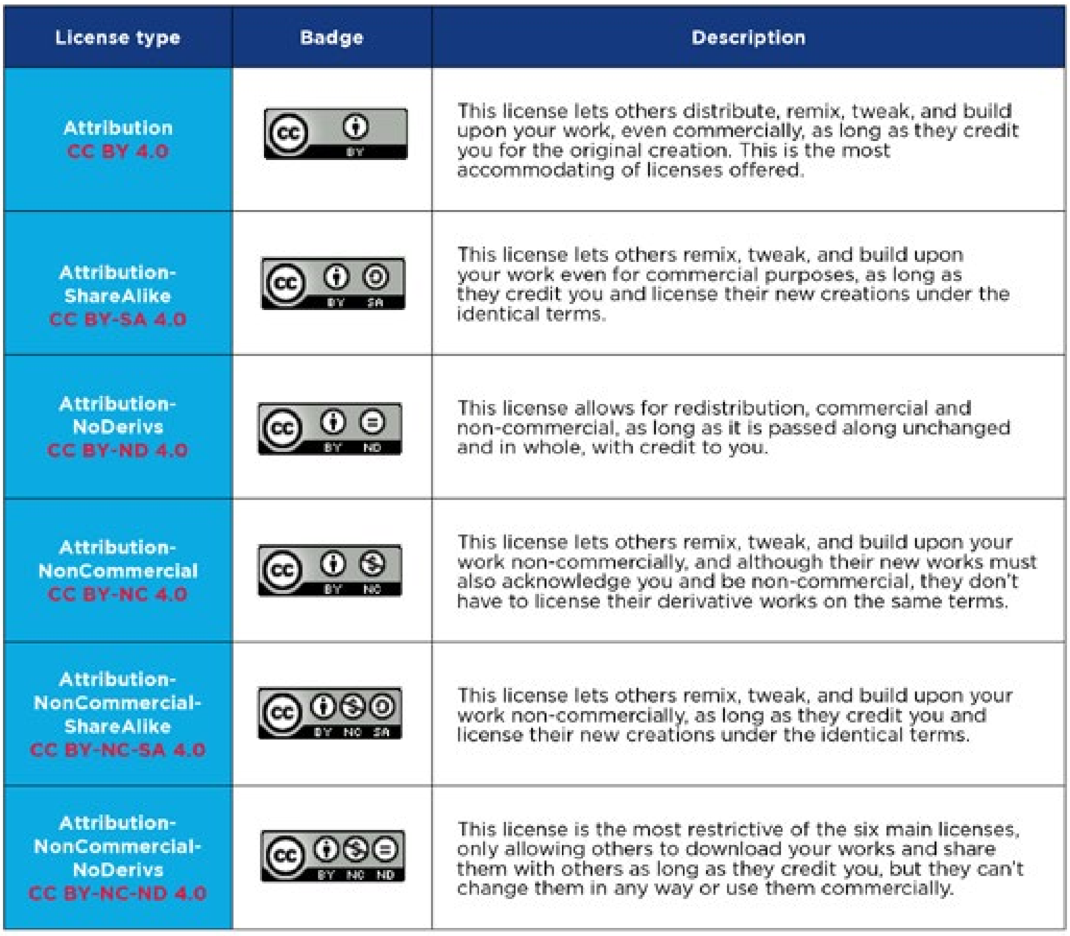
4.3.2.2 Data Custodianship/Sovereignty

As infrastructure assets often have multiple service providers managing the asset across the full lifecycle, it is critical that custodianship of the data is agreed to and clearly documented in associated metadata. This is a negotiation process between project partners and needs to be flexible and adaptable as new asset data is generated.

The data custodian holds overall accountability and responsibility for the dataset and is responsible for ensuring the collection or creation of data complies with legislative and policy requirements. The data custodian ensures that appropriate privacy, security and data quality protections are built in from the outset of the asset lifecycle. Further information on custodianship is available in the Data and Information Custodianship Policy.

Key considerations in relation to data custodianship are:

- Data sovereignty, including the need to provide appropriate protections under Australian law to maintain the rights of the Data Custodian to access, protect and maintain the security of the data, and the inclusion of appropriate measures to ensure notification of data breaches.
- Data custodianship should also be incorporated into contract arrangements to ensure data remains available for the life of the infrastructure. Contracts should specify who the data owner is, and create appropriate restrictions, controls and safeguards as to the roles and responsibilities of other entities. Other uses and users of the data should also be considered, and access arrangements across the data spectrum (from closed data to data that is shared in limited circumstances to publicly open) need to be established in line with agency data governance.
- Agencies should consider the value of data as an asset at all times, including the value of openly available data as a public asset. Creative Commons BY licensing (see Table 1) should be used for open data as per the NSW Open Data Policy.
- Intellectual property attribution in data and trained machine learning models may also need to be addressed in your contract arrangements. For more information, refer to the NSW Intellectual Property Management Framework.



License type	Badge	Description
Attribution CC BY 4.0	cc BY	This license lets others distribute, remix, tweak, and build upon your work, even commercially, as long as they credit you for the original creation. This is the most accommodating of licenses offered.
Attribution-ShareAlike CC BY-SA 4.0	cc BY SA	This license lets others remix, tweak, and build upon your work even for commercial purposes, as long as they credit you and license their new creations under the identical terms.
Attribution-NoDerivs CC BY-ND 4.0	cc BY ND	This license allows for redistribution, commercial and non-commercial, as long as it is passed along unchanged and in whole, with credit to you.
Attribution-NonCommercial CC BY-NC 4.0	cc BY NC	This license lets others remix, tweak, and build upon your work non-commercially, and although their new works must also acknowledge you and be non-commercial, they don't have to license their derivative works on the same terms.
Attribution-NonCommercial-ShareAlike CC BY-NC-SA 4.0	cc BY NC SA	This license lets others remix, tweak, and build upon your work non-commercially, as long as they credit you and license their new creations under the identical terms.
Attribution-NonCommercial-NoDerivs CC BY-NC-ND 4.0	cc BY NC ND	This license is the most restrictive of the six main licenses, only allowing others to download your works and share them with others as long as they credit you, but they can't change them in any way or use them commercially.

Table 3 Creative Commons Licenses[21]

Service providers should fully comply with all data management and ownership requirements of the Cloud Policy or equivalent.

4.3.2.3 Exclusive rights to use of data

All contracts and design processes should make clear that exclusive rights to use of data generated by NSW Government agencies cannot be granted.

Where fair to affected individuals and reasonably practicable, data about public activities of citizens that government agencies cause or facilitate to be generated should be treated as a public asset and made available as open data as widely as possible, for example NSW public transport patronage data. Further advice is available in the NSW Open Data Policy.

4.3.2.4 New datasets

A new dataset may be generated as part of an infrastructure initiative that is a combination of data from several sources. It is very important to define 'ownership' (through rights of control to the exclusion of others) of data sources and confirm this is clear to all parties so that respective rights of use of new datasets are clear and understood by all parties.

The creation of new datasets should consider all business perspectives, including technical, financial, commercial, and whole of life requirements (e.g. type of operational phase data) to inform what type of data needs to be procured.

Note that rights and obligations under NSW privacy laws (where personal and/or health information is involved), the GIPA Act, as well as the State Records Act apply to new datasets.

4.3.3 Data retention and destruction obligations

All government data held by a service provider should be contractually required to be returned to government (in a format specified by government) at the end of a contract, or when a service or relationship with a service provider is discontinued. The retention and destruction of data must be compliant with relevant legislation and policies including the State Records Act 1988.

Alternatively, evidence must be provided to government of data destruction if legal data retention requirements have been met and data destruction has been authorised. Contracts should make clear whether this also includes removing all data and artefacts, including knowledge, rules and machine learning models extracted from the data.

4.3.4 Data privacy and security

Contracts must ensure that no personal data can be used by service providers for a purpose other than what is specified in the contract. Service providers must limit their data collection to only the approved purposes agencies have specified.

Depending on the nature of the data collected and used, agencies may want to address monitoring and mitigation responsibilities for software and hardware vulnerabilities in their contract. If these vulnerabilities lead to data insecurity or privacy impacts, liabilities and responsibilities should be defined in the contract.

Refer to Section 7.4 Data Security for further information on specific requirements, including privacy by design, reporting requirements, the NSW Cyber Security Policy and information classification guidance.

5 Data Requirements

Clusters / agencies should understand what information is required about their infrastructure assets to support the organisation's strategic objectives. These requirements are typically identified through a combination of decisions that are driven by both internal and external business objectives and requirements.

The data and information required throughout the asset lifecycle (e.g. Data and Information Requirements) must be determined by the Agency for each stage of the asset lifecycle. Information is typically required to support governance, operational and asset related decisions. The data and information are used to assess performance against the organisation's objectives and to assist in lifecycle decision-making.

The agency must be able to clearly define what information is required as information deliverables, so that these requirements can be communicated to other stakeholders and suppliers / delivery partners. In some cases, this may include portfolio level data than is not tied to a particular asset e.g. at the demand/need stage.

Information models, which generate the data and information deliverables, are typically defined against the agency's information requirements. As per ISO 19650-1 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 1: Concepts and principles the relationship between information requirements and information models are outlined below:

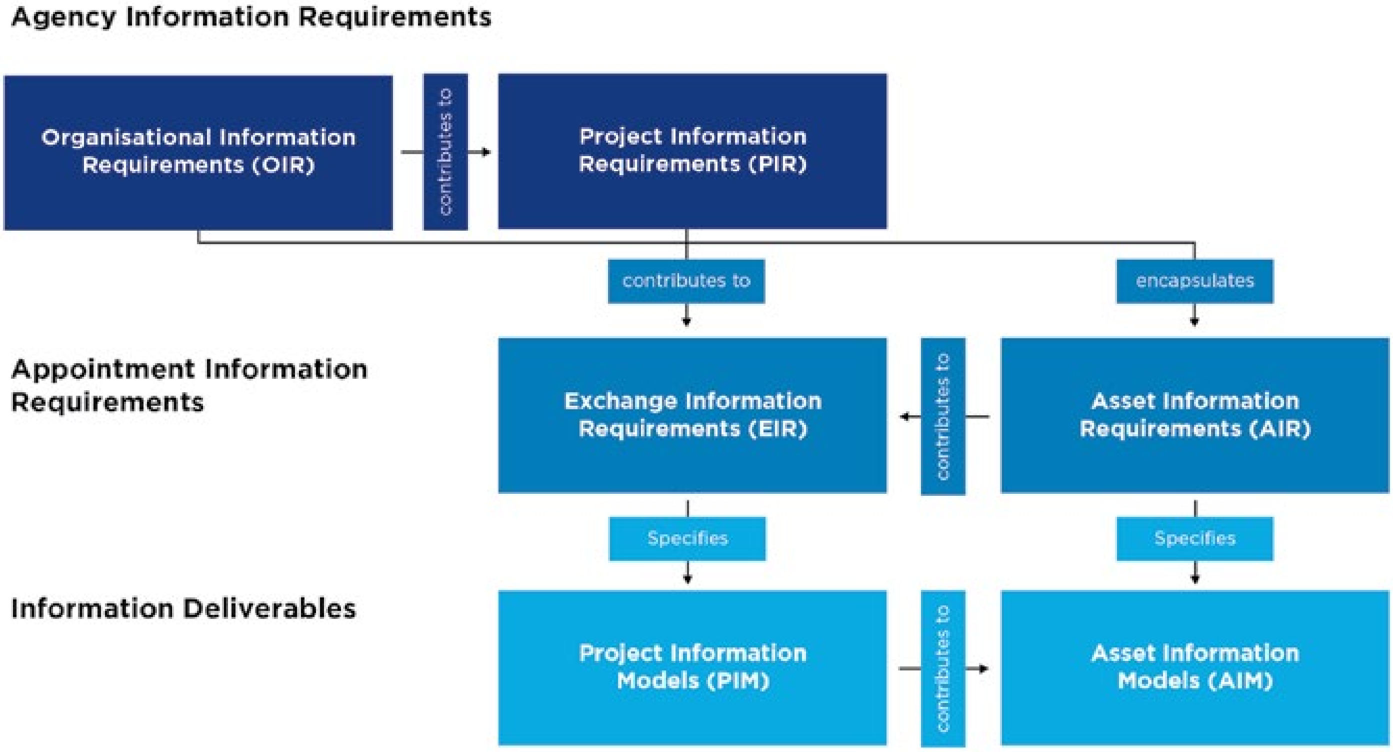

Agency Information Requirements
Organisational Information Requirements (OIR)
contributes to
Project Information Requirements (PIR)
contributes to
encapsulates
Appointment Information Requirements
Exchange Information Requirements (EIR)
contributes to
Asset Information Requirements (AIR)
Specifies
Specifies
Information Deliverables
Project Information Models (PIM)
contributes to
Asset Information Models (AIM)

Figure 11: Relationship between information requirements and models (adapted from ISO 19650)

In the context of infrastructure, information requirements can be defined as those data elements that need to be collected and analysed to provide the intelligence required about the infrastructure and its performance. The level of detail of data (geometrical and non-geometrical) and documentation also increases across the different stages of the asset lifecycle as illustrated in Figure 12:

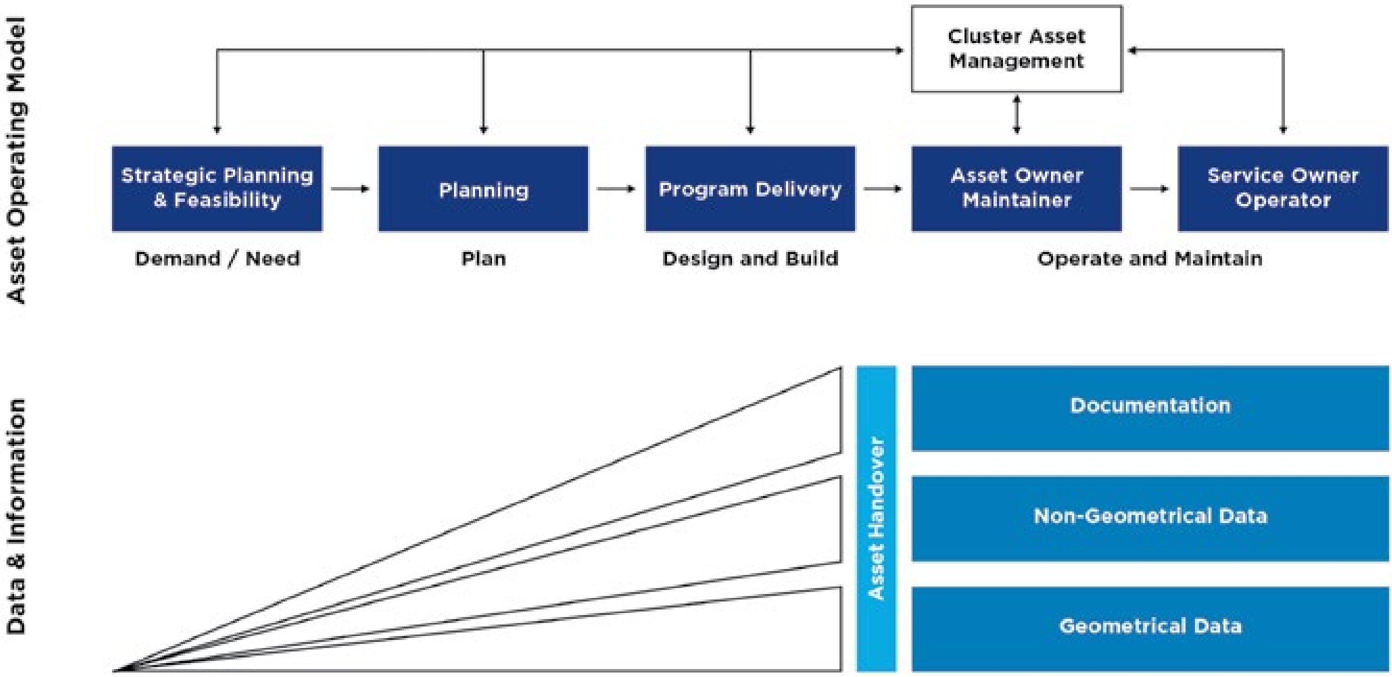


Figure 12: Increase in level of data across the asset lifecycle

5.1 Organisational Information Requirements (OIR)

Organisational Information Requirements (OIR) describe the information required by an agency for asset management systems and other organisational functions. That is, they are organisational-level business information requirements, such as whole of government reporting requirements and information required to assess progress against agency strategic plans, rather than asset-level or project-level information requirements.

The requirements at the OIR level typically support decisions that need to be made about the asset owned by the agency, including:

- Asset portfolio planning and management (e.g. understand the assets functionality, performance and cost)
- Strategic asset management
- Regulatory compliance.

Whole of government information management requirements are outlined in the:

- *State Records Act 1998*
- *Government Information (Public Access) Act 2009*
- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *Data Sharing (Government Sector) Act 2015*
- Information Management Framework

Additional legal or regulatory requirements apply in specific agency or business domains and all organisations should identify the specific requirements that apply to their environment. Requirements for information management are also outlined in agency-specific policies, standards and guidelines as well as in Commonwealth government legislation (for example *Security of Critical Infrastructure Act 2018*, *Telecommunication and Other Legislation Act 2017* (Telecommunications Sector Security Reforms).

Once these organisational level requirements are defined, the information requirements for the different phases of the asset lifecycle must be cascaded to the relevant parts of the business, including any external suppliers that support relevant business activities.

5.2 Project Information Requirements (PIR)

Project Information Requirements (PIR) set out and explain the information needed to answer or inform the strategic objectives of infrastructure projects. It conveys the OIR and agency project requirements to in-house teams and project-specific external suppliers setting out the information to be delivered for planning, design and construction of infrastructure projects.

Each agency will need to identify whether they prefer to define a single set of information requirements for projects, or whether there are subsets as outlined above. To align with the asset lifecycle and asset operating model defined in the IDMF, the following two sub-PIRs are defined.

5.2.1 Strategic PIR

Strategic Project Information Requirements cover the initial demand / need phase explaining the information needed to answer or inform high-level strategic planning objectives for infrastructure projects.

These strategic information requirements should extend to the level of precinct planning, which focuses more on higher level planning information requirements that support a range of cross agency activities, including population figures, functional benchmarks, operational concepts, etc.

Data requirements at these early stages should also start to define the functional data with regard to the aspects such as design specifications of an asset. This type of information supports the ability to measure performance and reliability over time to understand whether the delivered asset meets the original agreed to levels of service.

Even following approval to proceed to concept stages the level of detail is generally low, while mainly covering requirements for site investigations, ground data and schematic designs providing options for consideration during feasibility analysis.

5.2.2 Design and Build PIR

Design and Build Project Information Requirements explain the information needed to answer or inform the planning, acquisition, design and construction objectives for infrastructure projects.

The level of detail and volume of information increases during this phase of the asset lifecycle, with information requirements covering preliminary designs and systems requirements building up to a final business case phase. Following funding approval, the requirements cover detailed design, construction and as-built information requirements.

5.3 Asset Information Requirements (AIR)

Asset Information Requirements (AIR) set out the managerial, commercial and technical information elements required to produce asset information. It conveys OIR to project-specific external suppliers or in-house teams, setting out the information requirements of the agency in relation to the maintenance of infrastructure assets.

Each agency will need to identify whether they prefer to define a single set of information requirements to manage their assets, or whether to align with the asset lifecycle and agency asset operating model. To align with the agency operating model defined in the IDMF, the following two sub-sets have been defined, which also align with the development of operational and maintenance concepts during the project phase.

5.3.1 Maintenance AIR

The Maintenance AIR subset sets out the managerial, commercial and technical information elements required to manage the maintenance of an infrastructure asset or group of assets. It explains the information needed to answer or inform strategic, tactical and executional objectives for maintenance of the infrastructure. For larger projects where a maintenance concept is developed, it would be expected that these maintenance related requirements would be covered within the maintenance concept documentation.

The requirements should include information on the recommended maintenance plans and associated repair tasks that covers planned, preventative maintenance activities to support the owner / maintainer to anticipate and plan for resources and cost to maintain the assets.

The requirements captured in the AIR should also cover the renewal, repurposing, replacement, decommissioning and disposal of the assets.

5.3.2 Operations AIR

The Operations AIR subset sets out the managerial, commercial and technical elements of operating or providing a service utilising a specific infrastructure asset or group of assets, for example at the precinct level. Agencies will need to determine the appropriate level of aggregation of assets. It explains the information needed to answer or inform strategic, tactical and operational objectives in relation to the delivery of a service and the support provided by a particular asset or group of assets. For larger projects where an operations concept is developed, it is expected that these requirements would be covered within the operational concept documentation.

The requirements should include information on what is required to support normal operations of the asset to enable the owner / operator to anticipate the resources and costs to operate the assets.

5.4 Exchange Information Requirements (EIR)

Exchange Information Requirements (EIR) set out managerial, commercial and technical aspects of exchanging infrastructure data and information based on the project and asset information requirements. The EIR defines the information that will be required by the agency to be transferred between in-house project teams and external suppliers for the relevant phases of the infrastructure asset lifecycle.

A critical exchange is the asset handover process, e.g. the transfer of information from the Design and Build phases to the Operate and Maintain phase. This is the most significant transfer of information from one phase to the next during the asset lifecycle, which also poses the biggest risk of loss of information. The requirements for authorisation of data access change over the asset lifecycle.

For example, if you are approaching the market in the construct phase, access to some of the digital assets from the design phase may need to be available to organisations registered for the tender to prepare their responses. Once that stage is awarded, unsuccessful tenderers should be de-authorised and their read access cut off. Similarly for maintenance contracts, prospective tenderers will need access to the "as constructed" digital assets to prepare their responses, and then once awarded, the successful tenderer needs to be given read/edit access to the digital assets to maintain them as the physical infrastructure asset is maintained. Passing on of data from one phase of asset management to the next is important, and the use of standards between stakeholders and stages will help ensure the value of data is realised from stage to stage.

The information requirements then define the information model required for each phase of the lifecycle, noting that the project information models contribute to the asset information models, however not all data and information required for the construction of an asset is required to operate and maintain the asset.

6 Data Structure & Coordination

Infrastructure data that is well controlled and organised is more likely to be used across a variety of systems and provide value to organisations. The applications of structure to data through master data management, effective management of metadata and use of an appropriate data taxonomy and information model are key to enhancing the interoperability and value of infrastructure data.

When navigating the complexities and nuances of data structures and coordination, it is recommended to engage with relevant domain experts and authorities to ensure that good data management practices are adopted.

6.1 Master Data Management

Master Data Management (MDM) refers to processes used to define and manage master or reference data, including how it will be created, integrated, maintained and used throughout an organisation. Master Data Management is crucial in the government context because it seeks to ensure that agencies achieve consistency in master data 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: Master Data is interoperable across business units and agencies.
- Standardised: Master Data aligns with agreed state, national and international standards.
- Single view: Master Data is recorded and maintained on an accessible and, where possible, centralised repository creating a single view of the data.
- Controlled: changes to Master Data 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 Master Data – ensure its use in all appropriate business intelligence and analytics reporting across the organisation, at all levels.
- Establish maintenance policies and processes.

Additional resources

- 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.

6.2 Metadata Management

Metadata management is a foundational requirement for effective data management and refers to the maintenance of 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.

Metadata plays an important role in ensuring users can discover whether a data set is available, who the data custodian is, what the data means, and how accurate and reliable it is. Robust metadata management practices are required to ensure that data can be located, understood and used not only within agencies, but across government more broadly.

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 in 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. The following resources can be used for this purpose:
    - National Archives of Australia Minimum Metadata Set.
    - 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.
    - 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 19115:2015 – provides a standardised metadata format for describing geographic information and services. Note: An update to AS/NZS ISO 19115 is expected in 2020/21 to reflect time-dependent coordination of spatial information. In the interim, refer also to the ANZLIC Metadata advisory 'Preparing metadata for GDA2020 and the AGRS'
    - AS/NZS ISO 15836:2016 – establishes a standard for cross-domain description and defines the elements typically used in the context of an application profile.

- Measure current metadata effectiveness – this can be done by assessing your organisation's 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.

Additional 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.

6.3 Data Taxonomy

Taxonomy represents a formal structure of classes or types of objects within a knowledge domain by using a controlled vocabulary to make it easier to find related information. Defining and using a taxonomy can offer additional benefits in that users of the system will be categorising content and assets using a controlled vocabulary. This controlled vocabulary can be utilised as an integration reference point between different business systems.

A taxonomy must:

- Follow a hierarchical format and provide names for each object in relation to other objects.
- Have specific rules used to classify or categorise any object in a domain. These rules must be complete, consistent and unambiguous.
- Apply rigor in specification, ensuring any newly discovered object must fit into one and only one category or object.
- Inherit all the properties of the class above it and can also have additional properties.
- May also capture the membership properties of each object in relation to other objects.

A data taxonomy is a hierarchical structure separating data into specific classes based on common characteristics. The taxonomy represents a convenient way to classify data to prove it is unique and without redundancy. This includes both primary and generated data elements.

Taxonomies are different from metadata in that a taxonomy helps agencies to organise content and assets into hierarchical relationships. Classifying content and assets in a taxonomy can make it far easier to search for or browse an asset or content management system when agencies aren't sure exactly what they are looking for.

Organisations apply taxonomies to:

- Achieve better data quality.
- Organise metadata in an easy grasp format
- Manage data assets through data governance.
- Make it easier for a data steward to curate information.
- Guide machine learning and data experiences towards identifying trends and patterns.

6.4 Information Models

The term 'Information Model' is a description that is used for the collation of geometrical data, non-geometrical data, and associated documentation that represent infrastructure data at various asset lifecycle stages and states.

Data is driven by the creation of the Information Models required to support the project phases as well as the Operate and Maintain Phase. A key aim of the IDMF is the continuous development of asset data and information, including the re-use from one phase of the lifecycle to the next. This continuous growth in level of detail and handover from PIM to AIM is illustrated below.

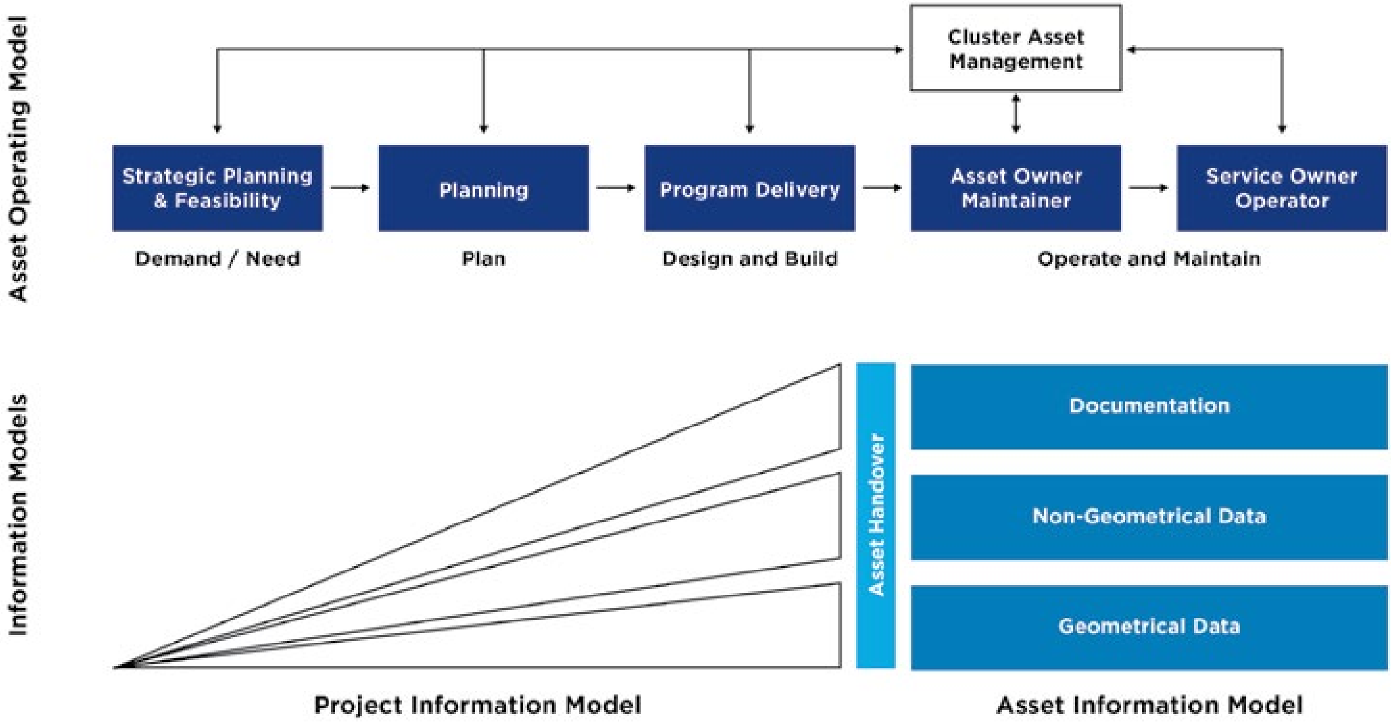


Figure 13: Level of information from PIM to AIM

Information models provide both geometrical and non-geometrical data and information, which includes 3D models, drawings, documentation and data such as asset registers. Information models should be consistent across an agency and must be able to be applied to a single infrastructure asset or a portfolio of infrastructure assets.

6.4.1 Project Information Models (PIM)

The PIM supports the delivery of the project, is a major contributor to the AIM, and is a collection of structured data produced during the planning, design and construction phases of the project. It is the overarching term given to all project and asset data generated during project planning and delivery, and includes all CAD, 3D / BIM Models, GIS, time, cost, quality, risk, etc., data. Where project planning and development is outsourced, this information is produced, managed and validated by an external supplier.

The supplier must transition the PIM to the Agency at the completion of the relevant contract as a consolidated deliverable for uploading into the relevant asset owner databases. This should include all environmental and contextual data that has informed the development of the design. In addition, it is critical that the PIM also includes the information required for operations and maintenance, including information such as building and building component warranties, guarantees, testing and commissioning data, etc.

The diagram below, *Figure 14*, illustrates how some of the project deliverables (e.g. 3D models, drawings and asset registers) change through the different stages of the project and asset lifecycles. It also shows some of the complexities involved in transferring information from the PIM to the AIM, for example the 3D Record Model contains all the information required during Operations and Maintenance and must reflect what was built, but it does not necessarily contain all the details required for construction.

All the design details required for construction are typically not required for operations and maintenance but do need to be archived as an As-Built Model for future reference. This information is useful when an asset is renewed or re-purposed.

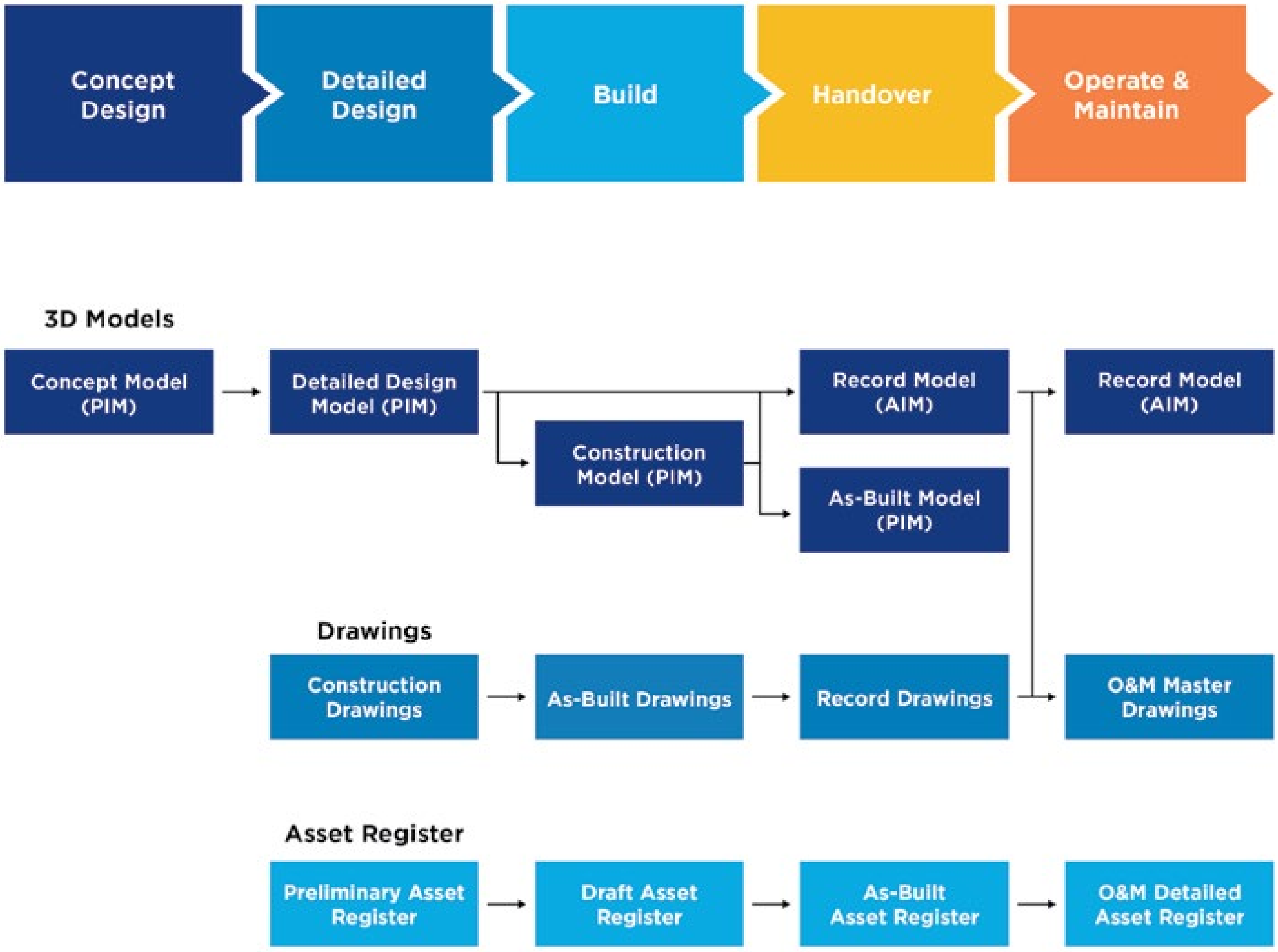


Figure 14: Models, drawings and registers from PIM to AIM

Based on the agency's asset operating model and how the information requirements have been defined, each agency will need to identify whether they prefer to use a single information model for projects, or whether there are different sub-models.

Two sub-models of the PIM are outlined to align with the asset operating model structure. The PIMs are progressively developed over the duration of the project to ultimately represent the full set of data and information required to build the project, which then also provides the major input to the AIM.

6.4.1.1 Strategic Project Information Model

The strategic sub-model of the PIM supports the delivery of the demand / need phase of the project, which extends from precinct planning through to concept design, and contributes to the sub-PIM used during the next phases of the project. It is the single source of information related to an infrastructure asset or assets developed that defines the options available to the agency to meet the requirements of the demand / need phase.

This model typically covers the business requirements, risks, existing conditions of the location of the planned infrastructure development, and also includes the options for the proposed design. Smarter infrastructure development requires increased levels of digital information earlier in projects, which makes the collection of near perfect existing condition survey data more important. The level and quality of the information collected during this phase of information model development also sets the baseline for future project phases.

6.4.1.2 Plan, Design and Build Project Information Model

The Plan, Design and Build PIM supports the delivery of the project and contributes to the AIM to provide the information required to effectively support asset management and operational activities. It is the single source of information related to an asset or assets developed during planning, acquisition, design and construction of a project.

The type of information captured by a PIM includes:

- Survey data (covering from existing conditions to as-built surveys)
- Documentation
- Risks
- 2D models and drawings
- 3D models
- Schedule information, including construction sequencing
- Cost estimates and actuals
- Asset data
- Visualisations, which range from animations through to videos and photos.

The PIM needs to provide the right level of information to support construction of the infrastructure assets, and ultimately support the ability to extract the AIM.

User Case Study: Digital Engineering reduces commercial risk for the Parramatta Light Rail

Digital Engineering (DE) makes use of processes that enable more productive methods of planning, constructing, operating and maintaining infrastructure assets. This case study focusses on the use of DE to improve the quality of underground utility surveys for the Parramatta Light Rail (PLR) Stage 1 project.

The PLR will connect Westmead to Carlingford via the Parramatta CBD. Experience from previous light rail projects highlighted that a lack of accurate information about underground utilities poses a significant risk to contractors.

As a solution to this, multiple parties were engaged to conduct surveys and gather details about the existing underground utilities. The application of DE was applied to develop a coordinated utilities model that was made available on a GIS system to potential tenderers. This allowed the NSW Government to provide bidding parties with accurate and reliable data.

6.4.2 Asset Information Models (AIM)

The AIM supports the strategic and day-to-day asset and operations management activities for both the agency (as asset owner) and operator. The AIM typically contains asset registers, maintenance planning information, cumulative maintenance costs, records of installation and maintenance dates, etc.

At the completion of the build phase, but prior to asset handover, the PIM is validated before forming the basis of the AIM. Upon compilation, the AIM must represent the asset as constructed, supplemented with the data as defined in the PIR that records the details of installation, testing and operational functional compliance.

The supplier is typically required to transition all of the Operations and Maintenance (O&M) information, models and associated datasets from the PIM into the AIM.

Three sub-models of the AIM are outlined below to align with the asset operating model structure. These sub-models of the AIM are developed to support both the maintenance and operations activities, which may be provided by different suppliers.

6.4.2.1 Maintenance Asset Information Model

The Maintenance sub-model of the AIM is a model that compiles the data and information required to support asset management and maintenance. It is the single source of information related to an asset or assets, at a level required to support an agency's asset management system.

This sub-model provides geometrical and non-geometrical data as well as relevant documentation. The maintenance AIM can be created from existing asset information systems, from newly generated information, or from information extracted from the PIM. The PIM should already contain the data requirements defined in a Maintenance Concept Document (MCD), as is typically developed for major infrastructure projects.

A maintenance AIM can include:

- Information, such as the original business requirements, i.e. what was the original design intent
- 3D models, which can be a combination of 3D spatial data of the environment and 3D design models
- Information, or links to information, about asset ownership, surveys, maintenance work that has been carried out, asset condition information, etc.

The Maintenance AIM should be managed within a CDE, which in the majority of cases, is a combination of different technology platforms including Enterprise Asset Management and GIS systems.

6.4.2.2 Operations Asset Information Model

The Operations sub-model of the AIM is a complementary set of information to the Maintenance AIM, with a specific focus on the operational aspects of delivering a service utilising the infrastructure assets as delivered by the project.

It is the single source of information related to the delivery of services utilising the asset or set of assets, with information captured at a level required to support an organisation's operational management systems. The Operations AIM may also be derived from the data requirements defined in an Operations Concept Document (OCD) as developed for a major infrastructure project.

The Operations AIM should be managed within a CDE, which may be using the same environment as the Maintenance AIM, but in many cases will be a separate set of technology applications.

6.4.2.3 Renew / Repurpose Asset Information Model

The Renew / Repurpose sub-set of the AIM is essentially an extract of information from the Maintenance and/or Operations sub-models that would be provided with an infrastructure asset that is to be renewed or repurposed. The requirements for the information to be provided in this sub-set would be determined by the early phases of a project, i.e. either the Demand / Need or Plan phase.

The Renew / Repurpose AIM would be the starting point for the creation of the next PIM as the single source of information to be handed over to a new asset owner, or to a project that is intended to renew or repurpose the infrastructure assets.

7 Data Management & Practice

Active application of good data management principles and practices is essential for the effective and efficient use of infrastructure data across the asset lifecycle. The information and data management approaches refined over years of application in the records and information management domain can be applied to asset data to provide cost savings and efficiencies in communication between stakeholders, and support use and reuse of the data for multiple uses.

7.1 Data management life cycle

The IDMF incorporates the key principles of the IMF into a schema designed to be applicable to infrastructure data across the asset lifecycle:

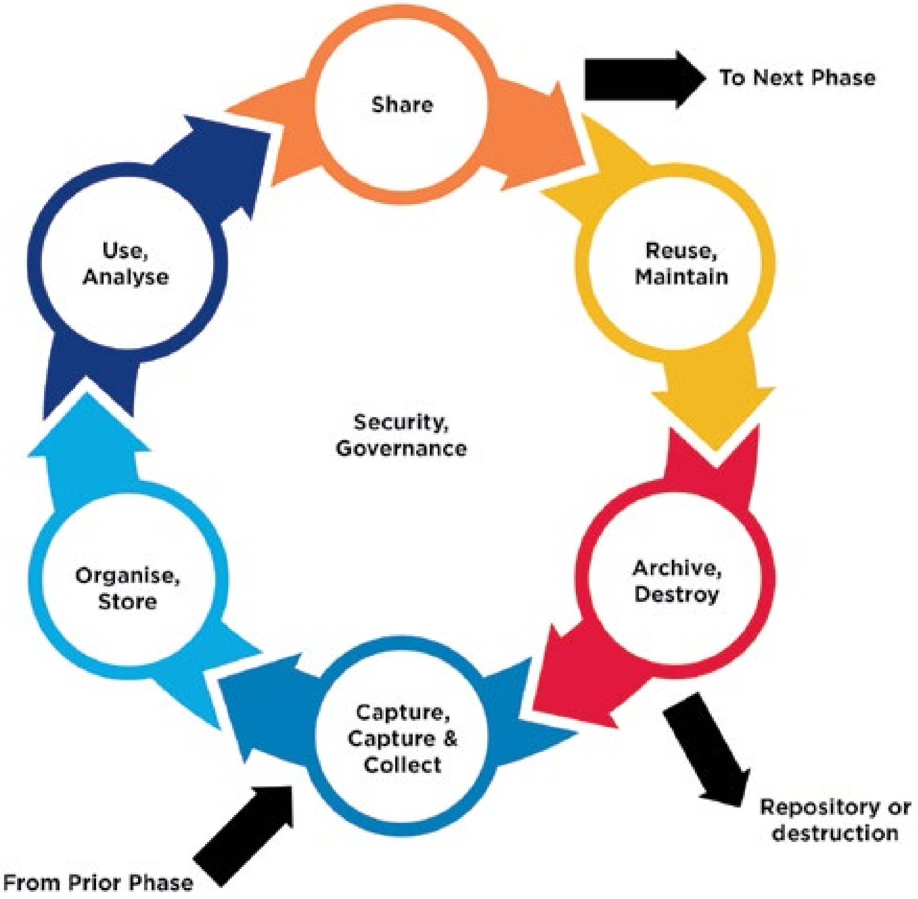


Figure 15: IDMF data management lifecycle

The two additional core features of the lifecycle that apply across each stage are governance and security.

The application of the data lifecycle as a standardised process across the life of an asset enhances communication between stages of the lifecycle, as different stakeholders inherit data from previous data custodians.

7.1.1 Create / Capture / Collect

The data management lifecycle begins with planning for the creation, collection, capture or acquisition of data. In the context of the IDMF, it is also the entry point for each stage of an asset's lifecycle, where data has been shared or inherited from the previous stage of the asset lifecycle.

7.1.1.1 Determine data needs and requirements across the asset life cycle

A key component of establishing an agency's infrastructure data management approach is to determine the infrastructure asset related information needs and requirements. The information requirements of the asset should be defined following Section 5 Data Requirements and be derived from the data that an organisation needs for strategic decision-making about an asset during its lifecycle.

Agencies should understand what information is required about their infrastructure assets to support the organisation's strategic objectives. These requirements are typically identified through a combination of decisions that are driven by both internal and external business objectives and requirements.

All requirements cannot not be known or planned for at the outset, but a structured approach from the beginning will assist in further definition as future requirements become known. Commencing planning with high-level forecasts will provide a valuable starting point for future development. Adopting the IDMF will allow for flexibility and adaptability – so imperfection at this stage is acceptable.

The information requirements will also need to be defined at each phase of the asset lifecycle. For example, when collecting data at the strategy and planning phase, high-level forecasts or assumptions may be sufficient, such as 20-year regional population projections or 10-year policy impact targets. These high-level forecasts or assumptions may be provided by reference to the NSW Common Planning Assumptions rather than being separately collected or defined. However, at the operating phase, real time occupancy and service data may be required.

For example, if the asset manager requires real time information on the number of people using the asset at any point in any location, the planners can ensure the right smart technologies are installed to capture this data.

7.1.1.2 Minimise data collection

It is important to have realistic, targeted information requirements and avoid asking for everything 'just in case'. Collecting more data than is needed to achieve the intended use of the data can create a data processing and storage burden and increase privacy and security risks. It is therefore important to consider the costs of collecting and maintaining such data against the benefits it will provide.

The data needed may also already exist. Before new data is collected or generated, it is important to check that it is not already available via NSW Government or other open data portals.

7.1.1.3 Determine the most appropriate collection method

Agencies should, wherever possible, minimise the use of manual data entry and rekeying by transition from the use of paper-based forms to online forms. This includes issuing paper-based work orders and forms for responsive maintenance, inspections etc.

Commonly used infrastructure data collection technologies include:

- Internet of Things (IoT) sensors – for example fibre optic, wireless, acoustic noise loggers, thermosensors and smart meters
- Imagery and measurement – for example, satellite and unmanned aerial vehicles/drones
- Closed Circuit Television (CCTV) and Video cameras
- Technologies such as Terrestrial Laser Scanning (TLS), Mobile Laser Scanning (MLS), Photogrammetry, Light Detection and Ranging (LiDAR) are being paired with legacy technologies to optimise and expedite data collection processes.

The use of smart ICT and the Internet of Things should be considered with reference to the Smart Infrastructure Policy.

7.1.2 Organise / Store

In order to support Asset Management, organisations must organise and store large amounts of data in an appropriate and efficient manner. The choice between storage options depends on many factors and is never one-size-fits all.

Storage environments should meet organisational information requirements (OIR), be compliant with relevant legislation and policies, be interoperable across different information management systems, and allow for the data to be stored and managed for the life of the asset.

Storage selection will be impacted by specific considerations, including:

- Intended use of the data (by whom and for what purpose)
- Characteristics of the existing database or information systems
- Type and volume of the data to be integrated
- The frequency the data will be accessed
- The frequency the data will be updated
- The speed at which data will need to be accessed, particularly in emergency situations
- Currently available technology

It is important to maintain a common environment for data storage. While data may be housed in a number of different source management/storage systems, a single portal can provide a single point of access that draws that data together for viewing and analysis. A single source of truth helps to avoid the duplication that results from storing the same data in different locations. Apart from the extra work needed to update data in multiple locations, duplication increases the risk that data will be amended in one location but not others, increasing the risk of incorrect or out-of-date information being used.

7.1.2.1 Design for Interoperability

Technical interoperability refers to the ability of different products or systems from different service providers to exchange information between each other so they can work together seamlessly, either in the present or in the future. It requires the use of standards between infrastructure, communication protocols and technologies that may be very different from each other, so that they can communicate with and across each other.

The NSW Smart Infrastructure Policy must also be followed for infrastructure projects subject to the Infrastructure Investor Assurance Framework (IIAF) and ICT Assurance Framework from 1 May 2020. The policy contains requirements relating to interoperability. Agencies should select open technology and/or vendor agnostic platforms where available and suited to agency needs. Agencies should also use open and recognised standards within and between the horizontal common layers of smart infrastructure.

Using open standards and platforms can improve an agency's ability to change the vendors it has paid to build and support the solutions. It can also reduce the cost of scaling to large numbers of devices and users of the solution. Additionally, it may increase the amount of alternate solution options available now or for future replacements/upgrades.

Use of Internet of Things (IoT) technologies in the infrastructure must also follow the NSW Government Internet of Things (IoT) Policy.

7.1.2.2 Ensure the storage environment is appropriate and secure

The level of security applied to data storage needs to be aligned with the sensitivity and security classification of the data. Infrastructure data may contain sensitive or security classified information, including legal and financial information. Agencies should follow the NSW Information Classification, Labelling and Handling Guidelines to determine the sensitivity or security classification of the data.

While most infrastructure data will not contain personal or sensitive information, it is important to check with agency privacy, security, data and/or legal experts before selecting a storage option. This is important because under the Privacy and Personal Information Protection Act 1998, data containing personal information will need increased security protection.

There are also storage obligations under the State Records Act 1998. For example, s 21 of the Act states that a person must not 'take or send a State record out of New South Wales' unless permitted under the provisions of s 21(2). In general, this requires permission or approval from NSW State Archives and Records.

However, there is a general authority that provides an exemption to keeping State records within New South Wales (GA35). This authority confirms that sending records for storage with, or maintenance by, service providers outside NSW is permitted provided that an appropriate risk assessment has been completed, and records are managed in accordance with all the requirements applicable to State records.

There may also be additional state or federal legislative requirements, particularly for critical infrastructure or telecommunications infrastructure. The Critical Infrastructure Centre website provides comprehensive guidance on Australian obligations for protection of critical infrastructure.

7.1.2.3 Data accessibility

Accessibility of asset data is not only an important management practice, it is also enshrined in the NSW Open Data Policy. The Policy states that data generated by government needs to be treated as a public asset and, where appropriate, made available as widely as possible. Making infrastructure data freely accessible allows other organisations and the public to benefit from, and innovate using, the data generated. However, it is recognised that risk-based judgements on security considerations need to be balanced against open data drivers. This needs to be done in the context of agencies' specific responsibilities under the Open Access Information provisions in Part 3 of the GIPA Act (for example, in relation to contract disclosure), as well as agency obligations in relation to access applications regarding infrastructure data that may be made pursuant to the GIPA Act.

It is important to align role-based or identity-based permissions with appropriate data classifications, and to recognise that not all data relating to an asset may be of the same classification and may require management of several different permission levels. For example, locations of security systems in correctional facilities, or drug storage in hospitals.

Whether data is made openly accessible or restricted access to trusted users, it is important the data is stored with supporting metadata, data quality and fitness-for-use statements, as well as measurement error and uncertainty estimates. This is important to enable interoperability and re-use.

7.1.3 Analyse / Use

Data analytics is a key part of the infrastructure management process because it allows large amounts of data to be transformed into useful information. Analytics can help identify and solve problems or predict issues that have not happened yet. For example, analytics can be used to optimise infrastructure management by enabling:

- more effective and efficient maintenance programs
- monitoring asset condition and performance
- identifying infrastructure gaps
- meeting minimum reporting requirements prescribed in legislation and policy
- ensuring effective capacity utilisation and planning.

7.1.3.1 Data Analysis

Data analysis should be fit-for-purpose. The type of analytics used will depend on the question being investigated. Data analytics used for infrastructure data can be reactive or proactive – these categories reside on a continuum from hindsight to insight to foresight (see *Figure 16*):

Reactive

Reactive analytics can assist organisations to respond quickly to operational issues or maintenance requirements.

- **Descriptive** – this form of analytics is applied to understand what happened to the asset e.g. past losses, enable loss forecasting and identify the cause of an incident.
- **Diagnostic** – this form of analytics is applied to find out why it's happening e.g. what process and conditions are creating the situation.

Proactive

Proactive analytics can assist organisations to better plan for the future needs of the asset users, or the asset itself.

- **Predictive** – this form of analytics is applied to predict what will happen to the asset and often uses machine learning algorithms.
- **Prescriptive** - this form of data analytics is applied to understand the best actions that can be taken in a particular situation to change the process operation.

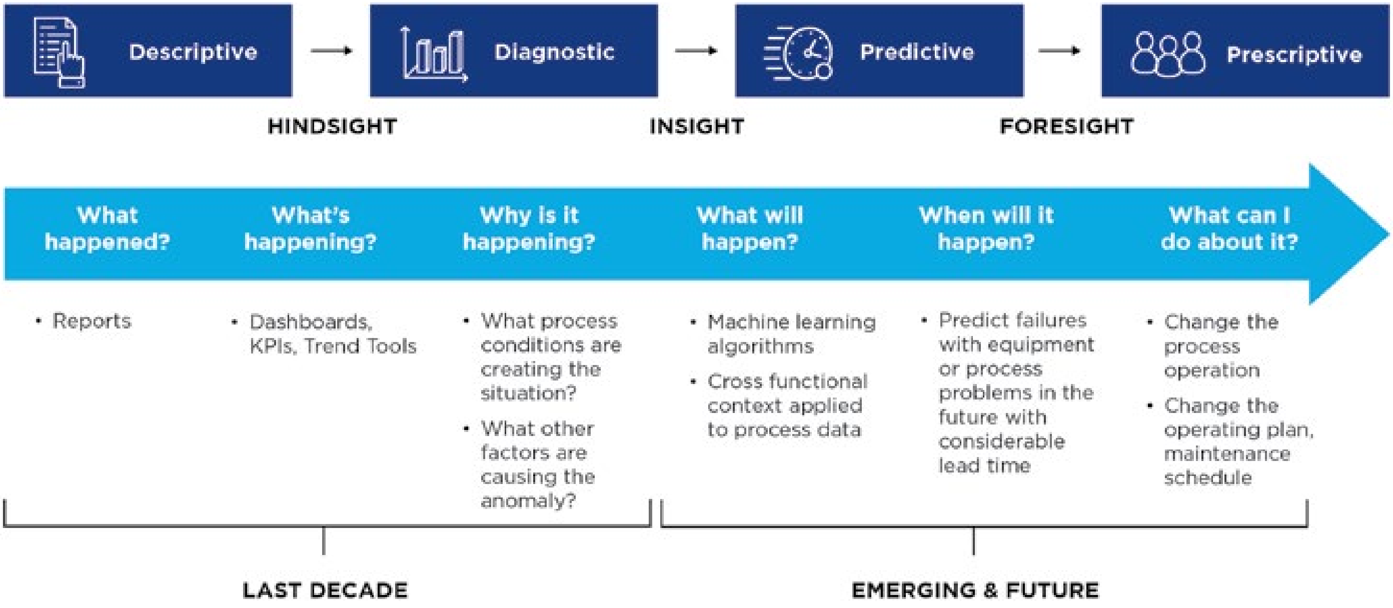

Descriptive
Diagnostic
Predictive
Prescriptive
HINDSIGHT
INSIGHT
FORESIGHT
What happened?
What's happening?
Why is it happening?
What will happen?
When will it happen?
What can I do about it?
• Reports
• Dashboards, KPIs, Trend Tools
• What process conditions are creating the situation?
• What other factors are causing the anomaly?
• Machine learning algorithms
• Cross functional context applied to process data
• Predict failures with equipment or process problems in the future with considerable lead time
• Change the process operation
• Change the operating plan, maintenance schedule
LAST DECADE
EMERGING & FUTURE

Figure 16: Data Analytics Continuum

7.1.3.2 Key data analytics concepts

7.1.3.2.1 Data Profiling

Understanding the profile of data includes assessment of quality and identifying potential issues with the data, including matching data formats against standards to ensure interoperability, identifying differences from expectations within datasets. Automated tools can be used to streamline these processes.

7.1.3.2.2 Data Cleansing

One of the first steps of analysing data (after defining the data requirements, collecting and storing the data) is to cleanse it. Data cleansing is vital for accurate data (incorrect data can generate misleading results). Analysing data and using techniques to automate these error checking methods can help to speed up this process, however a data analyst still needs to be involved to investigate any issues.

7.1.3.2.3 Data engineering and modelling

An analyst often needs to combine datasets and build models with multiple data layers to build data insights. Data modelling is when a data scientist builds a data model to correlate the data, often with business outcomes in mind.

7.1.3.2.4 Visualisation and communication of data

Communication is the last step of the data analytics process and is often overlooked. Data needs to be delivered to the organisation in a meaningful way to support decision making. Data visualisation is about the visual representation of data as a means of communication. For example, a common way to visualise infrastructure is via spatial systems like the enhanced 3D spatial platforms and digital twins.

7.1.3.2.5 Data usage for business objectives

Data generated or collected can be used to continuously track and measure many factors including usage, condition and exceptions. Without clear definitions of what constitutes success at each stage of the asset lifecycle, progress can lag, data collection and use can become costly and untargeted, and the value of infrastructure assets can be diminished over time.

Once immediate business objectives are delivered, leveraging data to identify new ways of operating and new service innovations can be explored. By combining various datasets and learning from previous infrastructure projects, infrastructure data can be used to develop data assets and innovations for use across the state to enable smarter infrastructure planning. Agencies should consider how asset data can be leveraged more effectively across their organisation or be made available for innovation as an open data resource.

7.1.4 Share

When working with data, it is important to remember that data can be closed, shared or open because of the sensitivity of the data, the level of risk associated with the data, and the permissions given on how it can be used and published. By understanding where data comes from, who can use it, and what can be done with it, the opportunities associated with sharing and using data can be optimised.

Benefits and safeguards in sharing data

Potential benefits:

- Improved understanding of infrastructure
- Improved decision-making
- Improved sustainability (productivity and efficiencies)
- Increased competition and innovation
- Improved network planning and resilience

Safeguards needed to share data relate to:

- Privacy provisions (collection of personal data)
- Intellectual property, liability and confidentiality
- Security
- Commercial considerations
- Technical issues i.e. quality and interoperability

The Data Spectrum diagram developed by ODI illustrates the differences between closed, shared and open data.

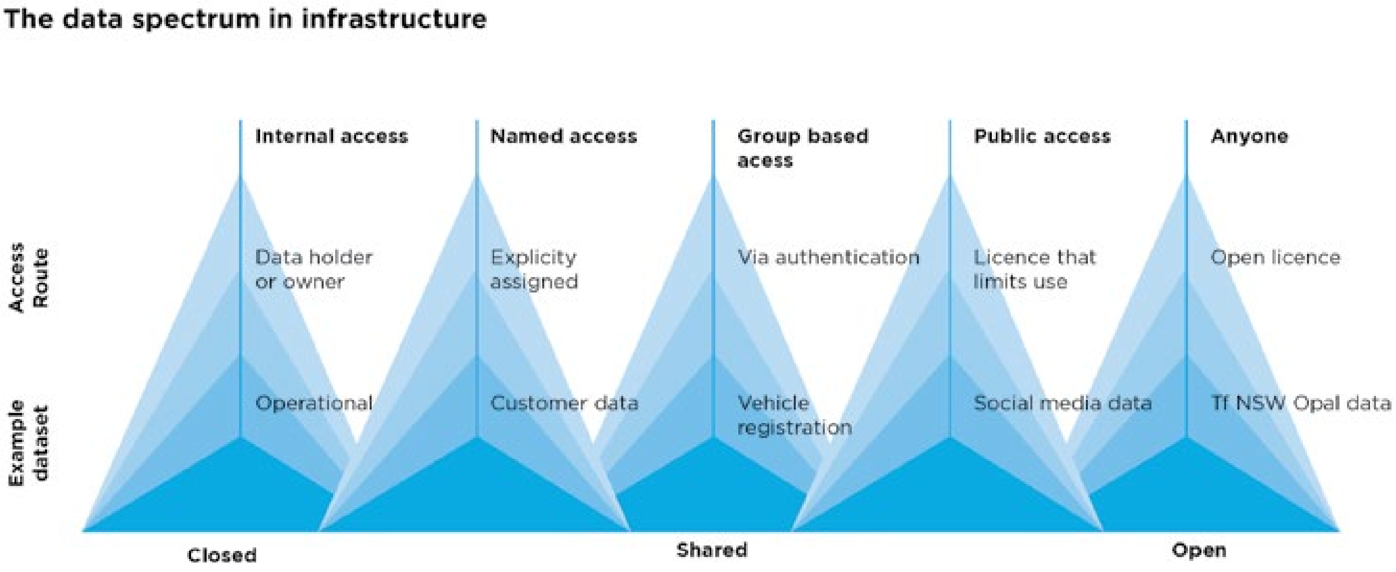


Figure 17: The data spectrum in infrastructure

Data sharing is a fundamental requirement for the management of most infrastructure assets. This is because on most infrastructure projects, there are numerous stakeholders that provide specialised services across the asset lifecycle. The need to exchange data between stakeholders in a timely and efficient way is key to the success of the asset's management. For example, the management of an asset relies on data exchange between a design team, a construction team, manufacturers and suppliers, as well as operation and maintenance teams.

Sharing of infrastructure data and other data across NSW Government is encouraged, provided appropriate protections are in place. The *Data Sharing (Government Sector) Act 2015* aims to remove barriers to data sharing within NSW Government, and to facilitate and improve government data sharing.

However, while NSW Government encourages the release of non-sensitive infrastructure data, the release of data should always take full account of security and privacy considerations. Guidance is available from the Information and Privacy Commission's guide on Data Sharing and Privacy.

Various arrangements can be made to between organisations to establish data sharing processes, including Memorandums of Understanding or Data Sharing Agreements. Further information is available at Data.NSW.

7.1.4.1 Closed or Secure Data

Closed or secure data is data that only people inside an organisation can see and use. National security, confidential business reports, and work emails are examples of data that organisations keep secure. There can be good reasons why data is closed and why closed data should not be available in the public domain.

From an infrastructure perspective, closed data is generally associated with sensitive or critical infrastructure or operations. The following references provide guidance on the ability to share (internally or externally to Government) infrastructure data:

- Federal government requirements on critical infrastructure assets in the *Security of Critical Infrastructure Act 2018*
- NSW critical infrastructure, including the ability to improve data sharing through the Trusted Information Sharing Network (TISN) for critical infrastructure resilience

Five Safes

The Five Safes model, developed by Felix Ritchie in the UK, provides a set of dimensions or 'safes' against which data disclosure risks can be assessed.

- Safe people: share data only with authorised users
- Safe settings: use data only in a safe and secure environment
- Safe projects: sharing data only for safe and authorised processes
- Safe outputs: ensuring data outputs do not identify people
- Safe data: applying appropriate protections to the data

These ideas have been adopted in Australia by the ABS, and by the Office of the National Data Commissioner, as Data Sharing Principles.

The Australian Computer Society has been working in conjunction with Australian governments and others to extend the model of the five safes (to ten safes) and is involved in the development of a Personal Information Factor (PIF) which measures the risk of re-identification of personal information in a deidentified dataset.

7.1.4.2 Shared Data

Shared data is data that is shared with a specific organisation, or group of organisations or people, for a specific purpose. Data sharing is how NSW government agencies can provide authorised access to the data they hold in a controlled manner, to help deliver better outcomes to the people of NSW.

Guidance on sharing of data is provided by Data.NSW, including the Five Safes, also referred to as data sharing principles.

The Commonwealth Data Sharing Principles help agencies to think about all of these factors together and better manage any risks associated with data sharing.

The five Data Sharing Principles (‘The Principles’) provide a framework for government agencies to share data safely:

- Share data for appropriate and authorised purposes
- Share data only with authorised users
- Use data in a safe and secure environment
- Apply appropriate protections to the data
- Ensure public outputs from data sharing projects do not identify the people or organisations in the data.

If the joint protections offered by the Principles are not sufficient to protect against the risk of data breaches or data re-identification, then the data should not be shared.

Data.NSW

Data.NSW is a NSW government initiative aimed at increasing the safe use of data across NSW government, to support better customer service, policy development, responsiveness and innovation. The guidance provided under the Sharing data section, includes:

- Data sharing principles
- Data sharing checklist for data owners
- Data sharing checklist for data requestors
- Making data safe for sharing and release
- Design and manage data for sharing and release
- Data sharing agreements and licences
- Requesting access to data
- Responding to agency data requests

The IDMF does not aim to replace any of this guidance, which is listed here for agencies to adopt, taking into consideration the level of openness (closed, shared or open) required for an agency’s infrastructure data, i.e. who can use the data and how.

7.1.4.3 Open Data

Open data is data that anyone can access, use and share. Governments and organisations have opened up access to data such as weather records, train timetables and real-time running, allowing others to use this data and discover new solutions for the benefit of all. However, simply releasing data is not sufficient and for data to be considered truly open, the owners must clearly state that other organisations or people can use it in any way they like, as without express permission, the data cannot be considered as open.

The NSW Government Open Data Policy is clear about its objectives and defines open data as follows: *“data is open to the extent that its management, release and characteristics meet the principles of openness”*.

In accordance with the Open Data Principles of the policy, agencies must manage data as a strategic asset to be:

- Open by default, protected where required
- Prioritised, discoverable and usable
- Primary and timely
- Well managed, trusted and authoritative
- Free where appropriate
- Subject to public input

A key component of defining information requirements for infrastructure must include defining. where on the data spectrum from closed to open the relevant infrastructure data fits.

7.1.5 Re-use / maintain

The re-use of existing infrastructure data assets for additional purposes will be one of the greatest sources of value for NSW government agencies, industry and the general public. Re-use of whole of government data assets such as those presented in the NSW Digital Twin will break down existing silos and artificial barriers to the use of information across cluster, administrative and jurisdictional boundaries. Re-use of data is facilitated by standards, interoperable data systems, common data formats and proactive sharing and release of open data.

Ongoing maintenance of asset data is a core process in infrastructure management. With the collection of large amounts of infrastructure data, it is essential to have processes in place to monitor, maintain and update the data to ensure the ongoing efficiency and improvement of the infrastructure asset. Specification of the frequency of update of data to align to organisational reporting requirements will reduce the friction associated with generation of ad hoc reports and data updates.

7.1.5.1 Ongoing monitoring of data assets

Continuous monitoring of the effectiveness of infrastructure data collection and use and management of changing requirements is needed throughout the asset lifecycle. Changes could be to the asset themselves, how they are managed, the technology supporting them, or the business requirements driving them, for example, changing stakeholder needs.

Asset owners need to reassess data governance approaches regularly in order to manage changes, privacy and security. This will ensure data is up to date when situations change, without becoming redundant and misleading. Data owners are typically accountable for ensuring that asset data is maintained and will need to establish an Asset Maintenance Schedule at the beginning of the project. This maintenance schedule should be implemented and monitored for the full duration of its life and include clear processes and points of accountability for maintaining and updating the data at each phase of the asset lifecycle.

7.1.5.2 Data validation

To sustain the required level of data quality, it is important to undertake data validation based on the requirements identified in the data needs assessment. Where possible, data validation should be automated, and errors corrected at the source. Data validation should also include the detection and mitigation of malicious data. Malicious content validation is important to protect not only the integrity of the data but also the system. Malicious data that is not blocked by data validation can be used to exploit vulnerabilities within a system and create an impact on other components in a system as well as other users.

7.1.5.3 Security considerations

Whether data is at rest, in use or in transit, there must be appropriate security controls in place to protect it. The security requirements of the data and systems may change over the lifecycle of the project, as the core data is updated with new data over time, and the risk profile of the data may change. It is therefore critical to assess risk changes and security requirements across the lifecycle. By assessing and re-assessing, the residual risks as well as newly identified risks can be mitigated with the appropriate controls. For more information, see the NSW Information Classification, Labelling and Handling Guidelines.

7.1.6 Archive / destroy

When an infrastructure data asset reaches the end of its life, the asset data should be archived or destroyed. To avoid large storage costs (or to minimise the risk of premature data destruction), agencies should assess and identify considerations that apply to the retention and destruction of data such as:

- Is there personal information in data assets? If so, under the Privacy and Personal Information Protection Act 1998 personal information should be destroyed as soon as the objective it was collected for is completed, in accordance with relevant requirements in the State Records Act.

  Note: Personal information may be required to be kept in some contexts, for instance, throughout an ongoing legal proceeding, and should be done so in accordance with the *Privacy and Personal Information Protection Act 1998.*

- Is there health information in data assets? If so, health information should be managed under the requirements of the *Health Records and Information Privacy Act 2002*.

- Data and records should be disposed of in accordance with NSW Information Classification, Labelling and Handling Guidelines. The Guidelines recommend records are disposed of with the same level of security that they are maintained. Guidance on de-identifying information is available from the Information is available from the Information and Privacy Commission.

- Are internal or external services dependent on the data?

- Are very large volumes of data involved? If so, it may not be economical to maintain the data for long periods of time. Approaches will be needed to routinely purge the data that is not needed for ongoing use.

- Are there any audit or accountability requirements applying to the infrastructure asst management process?

The State Records Act 1998 sets the rules for how long all government information needs to be retained. Depending on the type of infrastructure, the data asset will have different legal retention and destruction requirements. Agencies should refer to the NSW State Archives and Records website for more information. Any decision to archive or destroy data must also be made in accordance with the organisation's records and information management requirements.

All retention and destruction decisions need to be authorised and documented to achieve transparency and accountability over the destruction of infrastructure data assets. Governance and approvals must be defined in the agency's data governance documentation to ensure compliance with the State Records Act 1998, as well as with consideration of Government Information (Public Access) Act 2009 (GIPA) requirements. If working with multiple service providers, agencies should make sure they can all support and deploy the data retention and destruction frameworks required.

7.2 Data Quality

Once information requirements and relevant data standards have been identified, organisations need to decide on the quality of data required to ensure the data is fit-for-purpose. Data quality dimensions defined by the Data Management Association (DAMA) include:

Accuracy	Completeness	Consistency
Integrity	Reasonability	Timeliness
Uniqueness/de-duplication	Validity	Accessibility

Without a sufficient level of confidence in the data, an accurate view of the infrastructure and operations is incomplete, which may lead to poor decision-making.

As a general recommendation, preference data quality over data quantity. It is better to have a well-structured data set that has been verified and validated, and is reliable, than a large volume of poorly organised, unreliable data.

7.2.1 Data quality requirements

7.2.1.1 Data quality issues

Data quality issues caused by device breakdowns or device calibration can generate incorrect or inaccurate data which can lead to incorrect decision making. If this poses unacceptable business or customer risk, agencies should use their contract to define data governance requirements and required mitigations that minimise the likelihood of these risks. These can include service level agreements with service providers for fault identification, remediation and re-calibration of devices at regular intervals; acceptable standards for data quality; uptime and availability requirements; and consistency of data over time.

Data Quality Reporting

Data quality mechanisms should be built into the collection process and adhere to the NSW Government Standard for Data Quality Reporting.

Data should also be accompanied by a Data Quality Statement that outlines the quality of the data so it can be understood across the asset lifecycle. The NSW Government Data Quality Reporting tool can be used to generate a Data Quality Statement.

7.2.1.2 Liability arising from data quality

Agencies need to be transparent about any potential quality issues in licence or sharing agreements if the data will be made available to others as open data or as shared data. It may be important to flag in any contracts or sharing agreements that data may be incomplete, intermittently available or otherwise unreliable if there are connectivity or outage issues impacting your network. This will help protect against any liability claims.

Contracts, data licences and data sharing agreements must make clear that the NSW government is not responsible for any liability issues that may arise from data quality issues or reliance by users. NSW government organisations must be transparent about any quality issues and have high quality, routine, and well-governed processes in place to ensure the timeliness and accuracy of infrastructure data. This will mitigate against the likelihood of any impactful data quality issues occurring.

To guard against any liability issues that may arise with the use of a third-party product derived from NSW government data, agencies should seek legal advice on appropriate wording and include a disclaimer in any licence agreements. Disclaimers will not completely eliminate risk, but a combined metadata statement, licensing agreement and disclaimer is a suitable method for risk mitigation.

7.3 Data Integration

Data integration is the process of combining data from different sources into a single, unified view. To support the aims of NSW Government in supporting Smart Places and a NSW Digital Twin, agencies need to be aware of the requirements to integrate data from different sources. For instance, a typical GIS environment that is used to host a digital twin may not be able to consume and display a 3D infrastructure model without some form of transformation. Integration thus begins with the ingestion process, and includes steps such as cleansing, mapping and transformation. Data integration ultimately enables the analysis of federated models of information to support analytics tools that can produce effective, actionable business intelligence.

For infrastructure data, integration is the process of taking data from a number of disparate sources and making it usable. However, as the number of sources continues to grow the need for effective data integration becomes more important.

There are several key components of data integration relevant to infrastructure data, including:

- Data migration – moving data between locations, formats or applications;
- Application integration – enabling interoperability between systems;
- Master data management – creation and management of a single master reference for infrastructure data (supporting both the PIM and AIM)
- Data aggregation – combining different data sources, though either
  - Federation – combing data into a single dataset; or
  - Warehousing – physically combing data into a single physical database.

7.3.1 Data migration

Data migration is the process of moving data between locations, formats or applications. It is often caused by the introduction of a new system or location for the data. One common cause today is the shift from on-premises to cloud-based storage and applications.

This is also relevant to agencies when data is transferred to and from service providers, whether for a project (short duration), or for a services contract to outsource the operations and/or maintenance of state-owned assets (longer duration).

7.3.2 Application integration

Application integration is one approach to achieving interoperability between different business systems. Specifically, it requires approaching problems related to the organisational structure of an agency and arrangements with specific business partners. Some key factors to consider include:

- Interoperability – managing the different operating systems, including data formats so that they can be connected;
- Integration – creation of a standard process for managing the flow of data between applications and systems to ensure consistency; and
- Robustness, stability, scalability – regardless of the solutions implemented, it needs to be able to adapt to changes within the business environment.

Typical solutions also include middleware to help with centralisation and standardisation of data management.

7.3.3 Data aggregation

7.3.3.1 Data federation

Data federation is becoming increasingly important within the infrastructure space as it supports design activities such as clash detection, and O&M activities such as wayfinding when looking for specific assets to maintain.

Data federation typically creates a virtual database that does not store the source data, but contains information about where the actual data is. Regardless of how and where data is stored, it should be presented as one integrated dataset. This quite often implies that data federation involves transformation, cleansing, and, if necessary, enrichment of data.

7.3.3.2 Data warehousing

Data warehousing aggregates structured data from one or multiple sources in order to compare and analyse the data to achieve greater business intelligence. It is effective for getting a better understanding of the overall performance of infrastructure and associated assets because it makes a wide range of data available for analysis.

7.4 Data Security

Protecting the confidentiality and integrity of data, whilst maintaining the availability and accessibility of underlying systems, requires appropriate assessment and management of cybersecurity risks. Cybersecurity risks are events that could lead to unauthorised access, use, disclosure, disruption, modification or destruction of information, information technology, and/or operational technology. Cybersecurity risks should be considered as part of the broader business risk environment and align with the enterprise risk management strategy and practice of the agency. Agencies should also ensure that they are assessing and managing risks in their supply chain and for any other dependencies that exist.

Decision-making throughout the project lifecycle must be guided by risk management to identify mitigations and to avoid risks that are outside of the risk tolerance of the agency. Informed decision-making processes will help to manage the cybersecurity risk, although cybersecurity risk cannot be completely eliminated.

Agencies should also use a risk-based program to implement appropriate policy and technical controls (aligned to a recognised standard e.g. ISO 27001) to mitigate the risks identified. These programs should be implemented at the earliest stages of the procurement process and throughout the procurement and operational lifecycle of any ICT or OT system. Controls should be appropriately managed, governed and reviewed to ensure that they are performing as intended. Agencies must also identify other state and federal security obligations including the NSW Cyber Security Policy which contains mandatory requirements.

Developing a properly managed, risk-based approach to cyber security is vital for agencies to protect the data they are responsible for managing. This should extend to how and when data is shared with other agencies or with central data repositories, e.g. NSW Data Portal or NSW Spatial Digital Twin.

7.4.1 Implementing privacy by design

The protection of personal information is governed by the Privacy and Personal Information Protection Act 1998. Privacy by design and privacy impact assessments can help ensure privacy and innovation and provide a strong basis for data to be used anonymously.

Mapping the data flows of the infrastructure asset – who holds it and how they handle it at different stages of the asset lifecycle – can help identify any privacy risks inherent in the project and to implement privacy by design. It is important to monitor the creation, use and access to data to ensure appropriate and secure usage. Bolting on privacy protections at the end of the project is inadequate and may result in a security or privacy breach. For more information, refer to the NSW IoT Policy Privacy by Design guidance pp. 52-54.

7.4.2 Data and Security reporting requirements

Personal information is also subject to data and security breach reporting requirements. In NSW, the Information and Privacy Commission provides guidance to public sector agencies on data breaches and maintains a voluntary reporting scheme supported by policy and resources. Relevant requirements also include the Commonwealth mandatory Notifiable Data Breach Scheme (NDB) for entities covered by the Privacy Act 1998 and mandatory cyber incident reporting to Cyber Security NSW under the NSW Cyber Incident Response Plan, as required by the NSW Cyber Security Policy. There may be additional notification and reporting requirements relating to personal information as well as cyber security incidents.

7.4.3 NSW Cyber Security Policy

The NSW Cyber Security Policy includes the mandatory requirements all NSW government departments and public service agencies must adhere to, in order to ensure cyber security risks to information and systems are appropriately managed. The mandatory requirements encompass not only the risk management and cyber resilience of systems but broader organisational requirements around planning, governance, awareness, reporting and incident response. The NSW Cyber Security Policy applies not only to information and ICT systems but also Operational Technologies (e.g. Industrial Control Systems (ICS)) and Internet of Things (IoT) Devices.

7.4.4 NSW Information Classification, Labelling and Handling Guidelines

The NSW Information Classification, Labelling and Handling 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.

8 Data

Globally most organisations find it challenging to define the potential benefits of introducing new methods of working and technology in the built environment. One of the reasons why it is challenging to produce true figures about efficiency gains is that we have not started scratching the surface with regards to making infrastructure-related data usable, accessible and measurable. Data is also expensive, getting it right takes time, and getting it wrong is even more expensive.

Most of the currently available infrastructure data is unstructured and includes emails, documents, multimedia, video, PDF files, spreadsheets, messaging content, digital pictures and graphics. Whilst there is an emerging artificial intelligence (AI) industry developing algorithms enabling machines to make sense of the large amounts of infrastructure data produced across the asset lifecycle, large volumes of data are not machine readable, not interoperable, and not structured at all.

8.1 Infrastructure Data

The Project and Asset Information Models are a combination of geometrical (graphical) data, non-geometrical data and documents. This means that it is expected that for every component, product, material, and system that makes up any infrastructure and its associated physical assets, there would be some level of geometrical data, non-geometrical data, and associated documents. Figure 18: Information Models and Data illustrates this relationship between information models, information types, applications and file formats. Note file types are indicative only and should not represent endorsement of specific products over open file formats. A list of file formats accepted by the NSW Spatial Data Platform is at Appendix C – Standards.

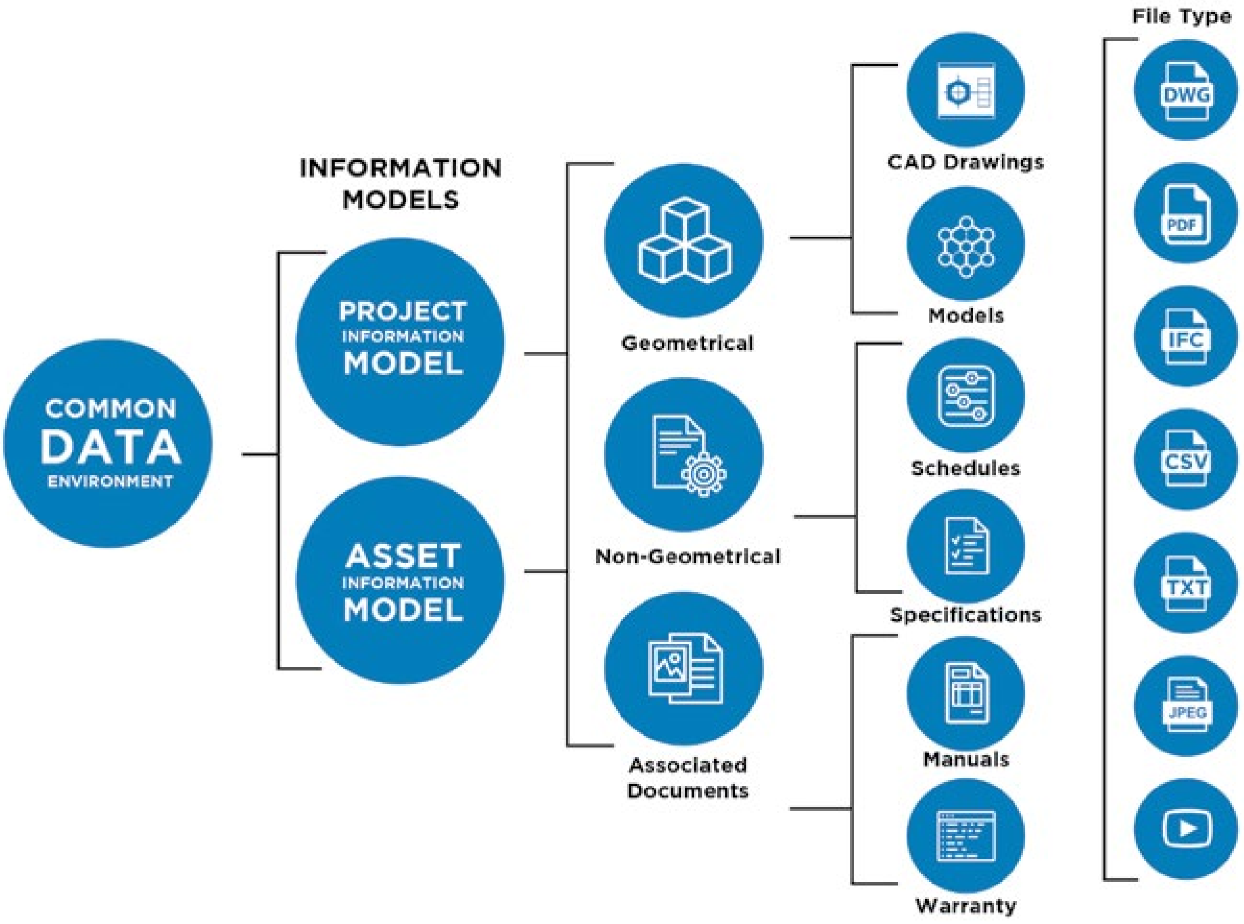


Figure 18: Information Models and Data

A key concept in the development of infrastructure data is the level of data definition required across the different lifecycle stages. ISO 19650 defines this as the “level of information need”, which states that “the quality of each information deliverable should be defined in terms of its granularity to serve the purpose for which the information is required and no more”. From an industry perspective, this information need is referred to as Level of Definition, where the amount of:

- Geometrical information developed for a given stage is termed “Level of Detail” or LOD, and
- Non-geometrical information developed is termed “Level of Information” or LOI.

AS ISO 19650-2 – *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) - Information management using building information modelling – Part 2:* Delivery *phase of the assets* details the typical requirements for each Level of Definition across the asset lifecycle. It explains what the information model can be relied upon for at each stage of development process as may be required to support co-ordination activities, logistics planning, programming and cost-planning. This then also determines the required detail within the 3D models developed by the project.

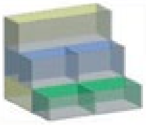
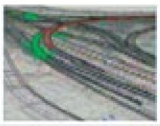
Lifecycle Stages	Strategic Planning /Planning	Design Concepts	Design	Build	Operations & Maintenance
Level of information need (AS ISO 19650)	2	3	4	5	6
LODev (BIM Forum)	LOD 100	LOD 200	LOD 300	LOD 400	LOD 500
Geometric Representation (Building Specific) (AS ISO 19650-2)					
Geometric Representation (Building Specific) (AS ISO 19650-2)					
Description (AS ISO 19650-2)	Models which communicate the initial response to the brief, aesthetic intent and outline performance requirements. The model can be used for early design development, analysis and coordination. Model content is not fixed and may be subject to further design development.	A dimensionally correct and coordinated model which communicates the response to the brief, aesthetic intent and some performance information that can be used for analysis, and early contractor engagement.	A dimensionally correct and coordinated model that can be used to verify compliance with regulatory requirements. The model can be used as the start point for the incorporation of specialist contractor design models and can include coordination, sequencing estimating purposes.	An accurate model of the asset before and during construction incorporating coordinated specialist subcontract design models and associated model attributes. The model can be used for sequencing of installation and capture of as installed information.	An accurate record of the asset as constructed at handover, including all information required for operation and maintenance.

Figure 19: Levels of Definition

Agencies need to be specific about the expected minimum levels of definition for project phases, as well as what is required for Operations and Maintenance. Note that LOD500 may not be required for all data developed during a project phase, as this level of information may not be required for operations and maintenance.

It is well understood that not all data is created equal – some data is structured, but from a data volume perspective, most is unstructured. The way the data is collected, processed and analysed all depends on its structure and format.

Structured data is comprised of clearly defined data types whose pattern makes them easily searchable; while unstructured data – "everything else" – is comprised of data that has no pre-defined format or organisation and is usually not as easily searchable. Unstructured data includes formats like audio, video and social media postings. In addition to being collected, processed and analysed in different ways, structured and unstructured data typically reside in different databases to structured data. Figure 20 illustrates the relationships between structured, semi-structured and unstructured data.

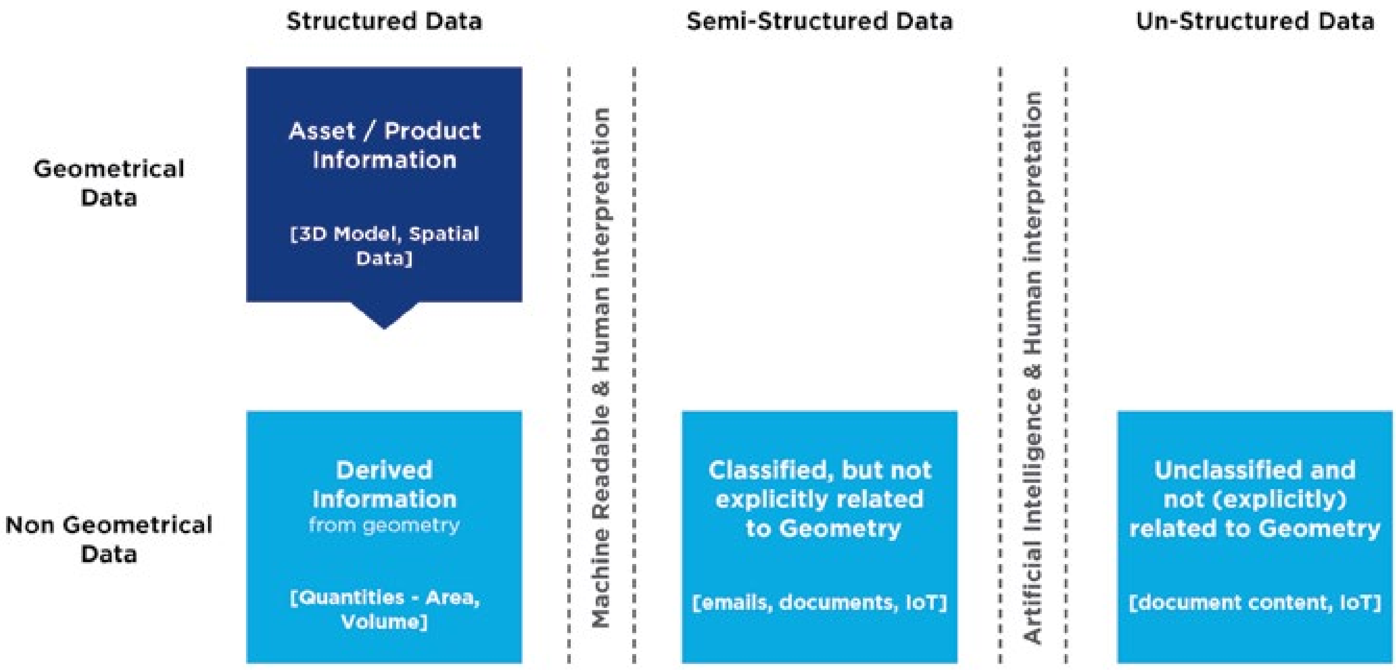

Structured Data
Semi-Structured Data
Un-Structured Data
Geometrical Data
Non Geometrical Data
Asset / Product Information
[3D Model, Spatial Data]
Derived Information from geometry
[Quantities - Area, Volume]
Machine Readable & Human interpretation
Classified, but not explicitly related to Geometry
[emails, documents, IoT]
Artificial Intelligence & Human interpretation
Unclassified and not (explicitly) related to Geometry
[document content, IoT]

Figure 20: Structured, Semi-Structured and Unstructured Data

Source: Adapted from "Non-Geometric Information Visualization in BIM: An Approach to Improve Project Team Communication" by Paula Gomez Zamora

There is no conflict between the use of structured and unstructured data, however agencies must be clear about their information requirements to define the most appropriate data structure, including the applications that use the data, e.g. relational databases for structured data, and many other types of applications for unstructured data.

What makes data management increasingly complex is the many disparate data sources, as well as the continuing rise in the volume of data – structured and unstructured. This is increasing the need for agencies to deal with both large volumes of data and large files (structured and unstructured).

The majority of infrastructure data currently available to agencies is unstructured. Unfortunately, the majority of the data currently captured and managed is not machine readable, not interoperable, and not well structured, if at all.

However, regardless of whether data is structured or unstructured, having the most accurate and relevant data available will be key for agencies looking to gain an advantage in making better whole of life decisions on their infrastructure. For overall success, agencies need to properly and effectively analyse all their data, regardless of the source or type to understand how best to maximise the value of infrastructure data.

8.1.1 Structured Data

Structured data is essential in all the stages of a built asset's lifecycle and the quality of the data must be consistently validated.

During the early stages of the asset lifecycle (Strategic Planning, Planning and Design), quality data is used to assist in decision making. Developing information models with structured data generates value driven data results that can be adapted and derived to provide the best possible outcome.

During the construction stage, structured data is used to ensure the values defining the performance of the products installed in an infrastructure asset meet the design and technical design criteria – it is key in developing the as-built model of an asset.

Based on the time and cost of infrastructure during the Operations and Maintenance stage, it is clear that quality data is critical to support activities such as maintenance scheduling, increasing efficiencies when replacing and upgrading parts, and measuring performance over a time period of actual versus proposed requirements.

8.1.1.1 Geometrical and Non-Geometrical Data

Structured geometrical data is spatial or object-based data (3D model or graphical representation) of the physical asset, while structured non-geometrical data (e.g. construction schedule) is derived and linked to a geometrical model. Structured data for infrastructure includes the following types of information:

- Geometrical data:
  - 2D CAD models
  - 3D Models (design, construction and as-builts, etc.)
  - GIS data sets
- Non-geometrical data (when associated with model geometry):
  - 4D schedule (time)
  - 5D cost (e.g. estimates)
  - 6D asset (for operations and maintenance)
  - Other linked data may include risk, health and safety, sustainability, etc.

Spatial and 3D model data is commonly visualised as geometry (lines, surfaces and solids) with parameters and other aspects of the model linked to it. Non-geometrical data could be derived directly from the model (e.g. areas) and stored in a database, or it could be extracted from an external database (e.g. from suppliers) and be stored in a dataset that is dependent on the geometry (e.g. materials for cost estimation).

What good looks like

- Clear, prescriptive information requirements (including data required) for infrastructure (for Projects and Operations & Maintenance);
- Identification of a common identifier to link all information, e.g. through adoption of consistent asset and location classification schemas, ideally compliant with ISO 12006-2 2015 Building construction – Organization of information about construction works – Part 2: Framework for classification and the NSW Standard for Spatially Enabling Information;

- Clear specifications on formats of geometrical and non-geometrical information deliverables, compliant with open international standards where available (see Appendix C – Standards);
- Consistent requirements for the exchange of information deliverables at a NSW Government and agency level, which can be consistently communicated to industry and service providers;
- Appropriate technology infrastructure that supports good data management practices, using open standards and architecture, open data exchange, access control and back up; and
- Internal data capabilities at NSW Government, agency and project level to view, review, share and store the structured information deliverables (e.g. via Common Data Environments).

How to achieve good practice

- Develop an agreed approach for infrastructure data management that aligns with the IDMF;
- Develop a standardised approach to structured (and non-structured) data across the asset lifecycle, noting that the approach depends on specific stage requirements;
- Incorporate data requirements in procurement processes;
- Utilise guidance and technical support for infrastructure data procurement; and
- Utilise data expertise to support projects, information handover and O&M.

8.1.2 Semi-structured Data

Some data used in an infrastructure context is neither structured nor unstructured. Semi-structured data maintains internal tags and markings that identify separate data elements, which then enables information grouping and hierarchies. Both documents and databases can be semi-structured. This type of data, which has critical business usage and value, is typically about 5-10% of the volume of structured, semi-structured and unstructured data. Examples of semi-structured data include:

- Email: Although more advanced analysis tools are necessary for thread tracking or concept searching the native email metadata enables classification and keyword searching without any additional tools.
- IoT sensor data: This type of data will increasingly require more attention from agencies to be better prepared for management of the large volumes of data generated by sensors. See the NSW IoT Policy for more guidance on the management of IoT data.

What good looks like

- Clarity on data governance for semi-structured data;
- Consistent requirements for the exchange of semi-structured information to ensure that agencies can engage appropriately with suppliers;
- Appropriate technology infrastructure to support management of larger volumes of semi-structured data, for instance, data lakes; and
- Data capabilities to manage, analyse and interpret semi-structured data.

How to achieve good practice

- Develop an agency approach to increase the value of semi-structured data by improving the classification and metadata of semi-structured data. This will ensure the semi-structured data is less prone to the “garbage in, garbage out” maxim.

8.1.3 Unstructured Data

Unstructured data is most often categorised as qualitative data and is difficult to process and analyse using conventional tools and methods. Unstructured data includes word processing documents, multimedia, video, PDF files, spreadsheets, messaging content, digital pictures and graphics, mobile phone GPS records, satellite imagery, and surveillance imagery. The challenge is that most of this data is used inefficiently. Significant industry effort is devoted to development of automated processes to make sense of the large amounts of data the construction industry produces.

Unstructured data is difficult to deconstruct because it has no pre-defined model, meaning it cannot be organised in relational databases. More than 80 percent of all data generated today is considered unstructured, and this number will continue to rise of technologies such as the Internet of Things. Finding the insight buried within unstructured data is often complex requiring advanced analytics (e.g. Artificial Intelligence) and a high level of technical expertise to really make a difference.

What good looks like

- Clarity on the uses and value of unstructured data to support agency infrastructure;
- Consistent requirements for the exchange of unstructured information to ensure that agencies can engage appropriately with suppliers;
- Appropriate technology infrastructure to support management of much larger volumes of unstructured data; and
- Data capabilities to manage, analyse and interpret unstructured data.

How to achieve good practice

- Develop an agency approach to increase the value of unstructured data by adopting appropriate methods and technologies, such as Artificial Intelligence, to support infrastructure management.

8.2 Big Data

Big data in a government infrastructure context may consist of records generated by IoT devices measuring external conditions, condition monitoring, service use, human or transport movement, or records gathered by facility, place or building management systems. Big data is characterised by:

- Volume: the quantity of generated and stored data.
- Variety: the type and nature of data.
- Velocity: the speed at which the data is generated and processed.
- Variability: the inconsistency of the data.
- Quality: the relevance and accuracy of the data.

Monitoring and analysis of live sensor data, captured as big data, will support a better understanding of performance during construction and operation, resulting in smarter designs, requiring less material, reducing carbon and needing less labour for construction, etc.

9 Implementation Guidance

The IDMF provides a framework for agency analysis, planning and alignment of infrastructure data approaches. It includes an approach to identifying, managing and using data over time, identifies policies and reference standards to be followed and provides guidance to agencies on the steps to be followed in data management.

Agency implementation of the IDMF will include a step-by-step approach to developing a suite of content that aligns broader organisational data management strategy with the information requirements identified in the IDMF for the management of infrastructure data.

Figure 21 summarises the inputs, controls, process and enablers identified in the IDMF that support the desired outcome of structured, consistent, secure, reusable and accurate infrastructure data. The direction and impact of each component should be established via desktop research and workshops including functional areas to fully identify existing organisational approaches and decisions where necessary.

Senior executive sponsorship and guidance will be needed in order to gain the support of teams across the organisation. This could be supported by the creation of a cross agency team to investigate and document inputs, controls and information requirements.

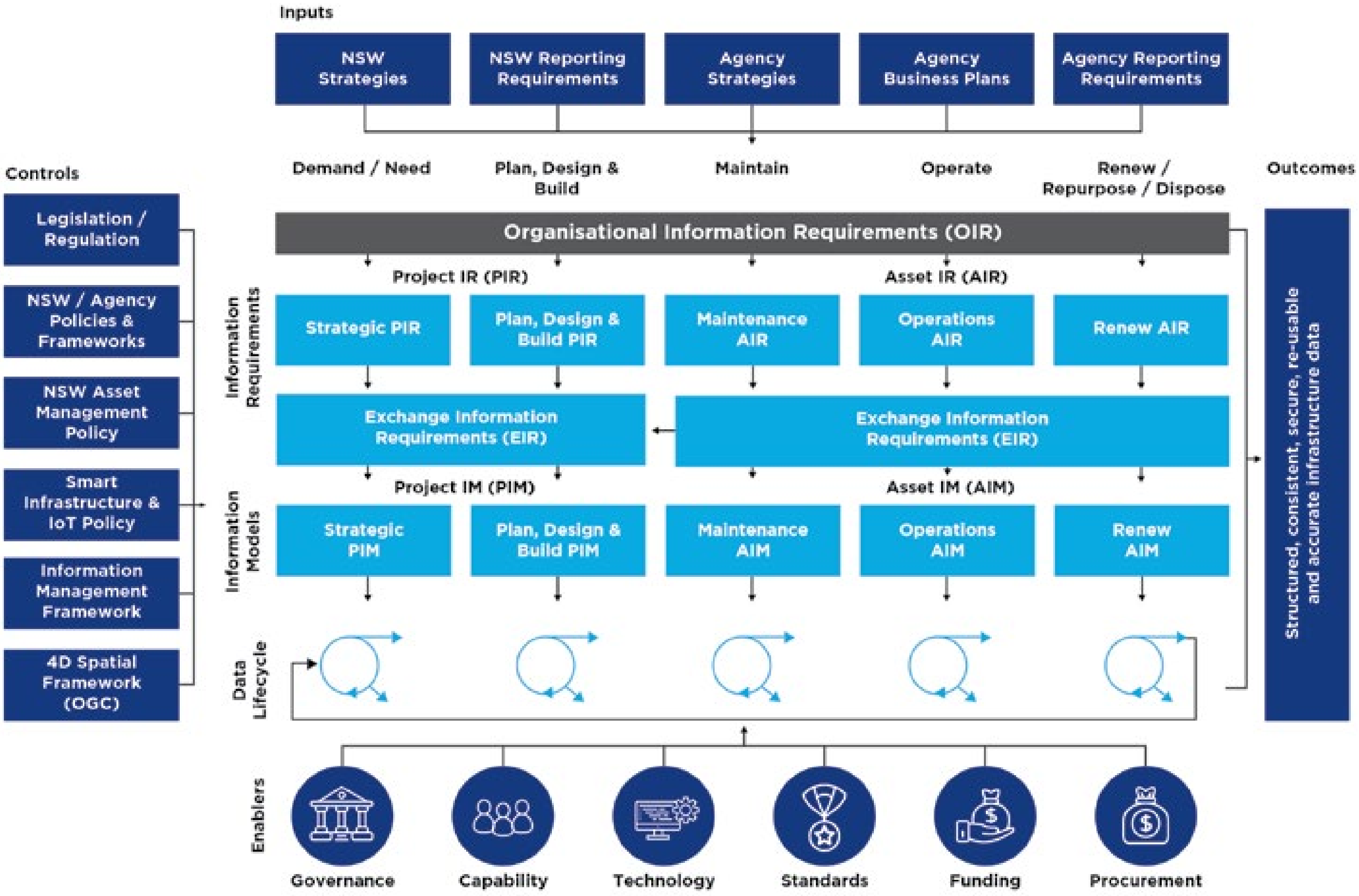


Figure 21: IDMF Context: Inputs, Controls, Process and Enablers

A strategic approach to infrastructure data management can significantly improve data assets over time, decrease delivery timelines, and improve insights into business opportunities, providing a substantial return on investment.

This approach could be documented in an agency specific Strategic Infrastructure Data Management Plan including:

- Clearly-defined agency vision of the value and use of Infrastructure Data
- Gap Analysis
    - Current-state & future-state of Infrastructure Data (linked to Asset Management / Digital Engineering Maturity Assessments)
    - Current-state and future-state reference architectures
- An Agency Infrastructure Data Management Framework
    - Data management maturity model and road map
    - Common data sets, structures and definitions
- Adoption strategy
- Integration strategies (for people, process, technology, and data)
- Communication plan

Further guidance, including minimum requirements to support cross agency data standardisation, inter-operability, and access and contribution to centralised data repositories will be developed over time. Additional templates will be also developed as part of the ongoing development of the IDMF to support agency implementation.

10 Next Steps

The IDMF is a living framework and suggestions for additional components are welcomed. Where additional components are identified, content development will continue to support agency implementation and capability uplift. The Smart Places Strategy, for instance, has identified additional policy work including the development of the following:

- **Data Protection Policy** to guide how data is collected, managed and stored as part of Smart Places implementation, including use of personal information factors.
- **Data as Asset Guidelines** to support agencies to invest in data as an asset, and to use data to inform investment decisions.

Additional components may include:

- A guide to measuring success of IDMF implementation against the overall objectives will be developed.
- A guide to estimating the financial impacts and cost of implementation
- Guidance on enhancing organisational capability
- High level data structure schemas
- Standardised procurement contract clauses
- Data sharing agreements – resources currently available at www.data.nsw.gov.au
- Future development of the Information Management Framework and Data Governance Toolkit available from www.data.nsw.gov.au.

Feedback on the IDMF is welcomed via datansw@customerservice.nsw.gov.au.

Appendix A – IDMF Project Background

The IDMF has been developed by the Data Analytics Centre at the Department of Customer Service (DCS). The DCS State Infrastructure Steering Committee, and the Smart Places Coordination Group has overseen the development, along with the following recommendations from the State Infrastructure Strategy 2018-2038:

- *Recommendation 28* – Develop a Data Infrastructure Ecosystem, starting with the Foundation Spatial Data Framework;
- *Recommendation 29* – Prepare a business case for upgrading the Foundation Spatial Data Framework from a map to a model (a real-time 3D model of the physical environment).
- *Recommendation 30* – Develop a Smart Cities Strategy and program business case;
- *Recommendation 31* – Develop a policy framework to guide investment in IoT and connected infrastructure; and
- *Recommendation 32* - Develop a policy and requirements for Smart Technology to be embedded in new and upgraded infrastructure.

The following agencies and organisations have been involved in the development, whether through participation in the Steering Committee, workshops, targeted consultation or interviews.

NSW Government Organisation	Division
Department of Communities and Justice	Digital & Technology Services
Department of Communities and Justice	Office of Emergency Management
Department of Communities and Justice	Justice Infrastructure
Department of Customer Service	Better Regulation Division
Department of Customer Service	Centre for Work Health and Safety
Department of Customer Service	Data Analytics Centre
Department of Customer Service	Digital.NSW
Department of Customer Service	Emergency Information Coordination Unit
Department of Customer Service	Information and Privacy Commission
Department of Customer Service	NSW Fair Trading
Department of Customer Service	Spatial Services
Department of Education	Schools Infrastructure
Department of Planning, Industry and Environment	ePlanning
Department of Planning, Industry and Environment	Land and Housing Corporation
Department of Planning, Industry and Environment	Property NSW
Department of Planning, Industry and Environment	Strategy and Reform
Department of Regional NSW	Geological Survey of NSW
Department of Regional NSW	Regional Growth Development Corporation
Greater Sydney Commission	City Planning Infrastructure
Infrastructure NSW	Asset Management
Infrastructure NSW	Strategy, Planning & Innovation

National Parks and Wildlife Service	Strategy and Coordination Branch
NSW Health	eHealth
NSW Health	Health Infrastructure
Sydney Water	Liveable City Solutions
Transport for NSW	Infrastructure & Place
Transport for NSW	Digital Engineering

Other Organisation	Division
Department of State Development, Queensland	Economic and Infrastructure Strategy
Department of Treasury and Finance, Victoria	Office of Projects Victoria
Standards Australia	Stakeholder Engagement
NatSpec	

Appendix B - Terminology

Term	Abbreviation	Definition
Agency		All Budget Material general government agencies and public non-financial corporations, excluding state-owned corporations and public financial corporations.
ANZLIC’s Foundation Spatial Data Framework	FSDF	Provides a common reference for the assembly and maintenance of foundation level spatial data across 10 themes: geocoded addressing, administrative boundaries, positioning, place names, land parcel and property, imagery, transport, water, elevation and depth, and land cover and land use.
Asset		All non-financial assets recognised by the agency including, but not limited to, land and buildings, plant and equipment, infrastructure systems, leased assets, works in progress, cultural and heritage collections, ICT systems and digital services.
Asset information requirement	AIR	Data and information requirements by the appointing party in relation to the operation of an asset.
Asset Information Model	AIM	Set of structured and unstructured information containers relating to the part of the lifecycle during which an asset is used, operated and maintained.
Asset lifecycle		All the stages an asset experiences over the period from conception to end-of-life or contract and typically would include planning, acquisition, delivery, operations and disposal.
Asset Management Framework		The set of interrelated or interacting policies, objectives and processes required to achieve the agency’s objectives through the management of existing and planned assets. The term and definition of ‘Management Framework’ is interchangeable with that of ‘Management System’ as used in the International Standard for Asset Management (ISO 55001).
Asset Management Policy (for the agency)		An authoritative statement of leadership commitment to effective asset management and sets the direction for asset management within the agency.

Asset management		Asset management is the coordinated activities of an organisation to realise value from asset(s). Asset management is a suite of activities that enable physical and non-physical assets to deliv-er the value they were designed to deliver. Asset management typically involves an asset management system. The system will ensure resources, the competence, the awareness, the communication, the information requirements and the documented information are all enabled and focused on enabling the value that asset management delivers from the assets.
Asset owner		The individual, entity, or organisation responsible for asset management policy, strategy, plan-ning and decision-making for optimising the cost, risk and performance of assets over their lifecycle. Note: ownership of physical and non-physical assets may differ over the lifecycle of the asset.
Asset portfolio		The collection of assets within the scope of the Asset Management Framework. For the pur-poses of this policy, the asset portfolio covers all non-financial assets recognised by the agency including, but not limited to, land and buildings, plant and equipment, infrastructure systems, leased assets, works in progress, cultural and heritage collections, ICT systems, and digital services.
Australasian BIM Advisory Board	ABAB	Links industry leaders and expertise from government, industry and academia, and promotes best practice and consistent approaches to BIM practices, standards and requirements.
Australian and New Zealand Land Information Council (ANZLIC)	ANZLIC	Also referred to as the Spatial Information Council, ANZLIC is the peak intergovernmental body providing leadership in the collection, management and use of spatial information.
Budget Material Agencies		All entities considered material for whole-of-government purposes, which are controlled by the NSW Government and the Government Finance Statistics sectors under which they are classi-fied. A list of Budget Material Agencies is typically published in the NSW Budget Papers.
Building information modelling	BIM	Use of a shared digital representation of a built or to be built asset to facilitate design, construc-tion and operation processes to form a reliable basis for decisions.
Built environment		All types of buildings (e.g. residential, industrial, commercial, hospitals, schools), all built infrastructure (e.g. roads, rail, utilities) and the urban space and landscape between and around buildings and infrastructure (e.g. precinct).

Capital project		A project primarily comprised of one or more of the following elements: - Infrastructure - Equipment - Equipment - Property developments - Property developments - Operational technology that forms a component of a capital project.
Clusters		The administrative arrangements that bring together a group of different legal and administrative agencies and allow similar and complementary government services to be coordinated more effectively within a broad policy area.
Common data environment	CDE	Agreed source of information for the whole asset lifecycle used to collect, manage and dissemi-nate all relevant approved project documents for multi-disciplinary teams in a managed process. Pairing a CDE with DE processes enhances collaborative information flow, which can be readily leveraged from one phase of the asset lifecycle to the next. Note: A CDE may use a project server, an extranet, a file-based retrieval system or another suitable toolset.
Community infrastructure		System of facilities, equipment and services that support the operations and activities of communities.
Computer-aided design	CAD	A geometric/symbol-based computer drawing system that replicates hand- drawing techniques. CAD software can prepare 3D lines, surfaces or solids that are suitable for presentation on hard-copy plots of drawings, and/or as background data for other 3D data or BIM.
Computer-aided facility management	CAFM	The support of facility management by information technology.
Construction Operations Building infor-mation exchange	COBie	Structured facility information for the commissioning, operation, and maintenance of a project often in a neutral spreadsheet format that is used to supply data to the asset owner or operator to populate decision-making tools, facilities management, and asset management systems. COBie can facilitate transformation from document-centric to information-centric handover pro-cesses to facility and asset operator's post-construction.
Data Sharing Principles		Risk management safeguards applied when sharing public sector data.
Data		Information represented in a manner suitable for automatic processing.

Data Custodian	The Agency, body or position designated with the Custody of a specified Dataset or Information asset. The custodian is primarily responsible for: • the development, management, care and maintenance of a specified Dataset or Information asset; • ensuring that all legal, regulatory and policy requirements are met in relation to the management of the specified Dataset or Information asset; and • determining the conditions for appropriate use, sharing and distribution of the specified Dataset or Information asset.
Data Owner	This term is often used interchangeably with 'Data Custodian'.
Delivery Agency	The Government agency tasked with developing and / or delivering a project applicable under this Framework and the NSW Gateway Policy.
Department	A Department within the meaning of the Government Sector Employment Act 2013.
Digital 3D/4D cadastre	A digital model of cadastral boundaries and properties that defines, records and delivers land parcel information in support of tenure (ownership), land use and land value. The 3D element comprises transformation of the current 2D cadastre with elevation data such that the cadastre includes a height dimension. The 4D element involves creating temporal cadastral parcels that include historical and future data.
Digital Engineering	convergence of emerging technologies such as Building Information Modelling (BIM), Geographic Information Systems (GIS) and related systems to derive better business, project and asset management outcomes. Digital Engineering enables a collaborative way of working using digital processes to enable more productive methods of planning, designing, constructing, operating and maintaining assets through their lifecycle. [NDEEP]
Digital model	A three-dimensional representation in electronic format of infrastructure elements representing a combination of solid objects and specially located data with true-to-scale spatial relationships and dimensions. A model may include additional information or data. Also known as digital twin/ BIM model / data rich 3D model.
Digital twin	A dynamic digital representation of a real-world object or system.

Digital twin ecosystem		Interoperable data and connected digital twins governed by authentication and authorisation rules to enable role-based access to securely shared data.
Employer		Individual or organisation named in an appointment or project contract as the employer. Receiver of information concerning works, goods or services from a lead appointed party.
Equipment		The necessary assets used on or to support an infrastructure system and can include fleet and rolling stock.
Exchange information requirement	EIR	Specification for data and information by the appointing party that the appointed party is ex-pected to meet during the appointment.
F.A.I.R. (Findable, Accessible, Interoperable, Reusable) Principles	FAIR	Designed to ensure users can find, read, use and reuse data.
Federated model		A group of systems operating in a standard, collective and connected environment.
Industry Foundation Classes	IFC	A specification for a neutral data format to describe, exchange and share information typically used within building and facility management industry sectors. IFC data model consists of definitions, rules and protocols that uniquely define datasets, which describe capital facilities throughout their lifecycles. IFC is the only non-proprietary, open global data model specification available.
Information and Communications Tech-nology	ICT	The common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use such as stand-alone Operational Technology projects.
Information model		Set of structured and unstructured information containers. This can relate to the operational phase or the delivery phase of a built asset i.e. a project information model or an asset infor-mation model respectively. Information models may include geometrical models, schedules, databases, etc. Unstructured information containers may include documentation, video clips, sound recordings etc.

Information		Knowledge concerning objects, such as facts, events, things, processes or ideas, including concepts, that within a certain context, have a particular meaning. Information is data that has been processed into a form (physical, oral or electronic) that is meaningful to the recipient). This definition includes but is not limited to: • raw data; • information that has been produced by combining or adding value to raw data; • images; • audio-visual material; • web content; • records; • metadata, policies and procedures; • methodologies; • dashboards; • models; • analysis; • knowledge; and • strategies.
Information Asset		A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information Assets have recognisable and manageable value, risk, content and lifecycles.
Infrastructure		The basic economic and social services, facilities and installations to support society including water, wastewater, transport (including road, rail, ports, airports etc), sport and culture, power, communications, digital and data, police and justice, health, education and family and community services.
Infrastructure data		Data or information relating to the planning, design, construction, operation and maintenance of infrastructure.
Infrastructure data management framework	IDMF	This document.
Infrastructure New South Wales	INSW	
Infrastructure NSW Assurance Team		The dedicated team within Infrastructure NSW responsible for implementing and administering the IIAF including organising Reviews.

Infrastructure NSW Reporting and Assurance Portal		Online portal administered by Infrastructure NSW for the management of IIAF functions.
Intellectual property	IP	The results or output of intellectual activity and creative effort. IP assets are intangible, and their economic value exists largely in the set of exclusive rights that an owner has in the asset. IP may be protected through copyright, trademarks, patents, designs, circuit layouts and plant breeder's rights.
International Organization for Standardisa-tion	ISO	An international standard-setting body composed of representatives from various national stand-ards organisations.
Internet of Things	IoT	IoT refers to physical devices that are connected to the internet, collecting and sharing data. It is the global network of infrastructure, vehicles, wearable devices, home appliances, medical technologies and other objects that are embedded with electronics, software, sensors and actua-tors, enabling these 'things' to share and exchange data to perform their functions more efficient-ly and effectively.
Level 2 BIM		A level of maturity in BIM, which is distinguished by collaborative working. It involves developing asset information in a collaborative data-rich 3D environment created in separate discipline mod-els. The collaboration is in the form of information exchange processes specific to a project and coordinated between different systems and project participants.
Natural environment		All living and non-living things that occur naturally, meaning not because of humans. This in-cludes ecological units such as vegetation, microorganisms, soil, rocks, atmosphere and natural events, which are natural systems without much human interference, as well as universal natu-ral resources, such as climate, air and water, which lack clear-cut boundaries.
Open data		Data that is freely available, easily discoverable and accessible, and published in ways and un-der licences that allows use without restriction from copyright, patents or other control mecha-nisms.
Operational technology		Can include systems that relate to service delivery, such as tolling systems, rail signalling or technology to support a new school or hospital.
Organisational information requirement	OIR	Specification for what, when, how and for whom information is to be produced in relation to or-ganisational objectives.

Project		A temporary organisation, usually existing for a much shorter duration than a program, which will deliver one or more outputs in accordance with an agreed business case. Under the IIAF a capi-tal project is defined as infrastructure, equipment, property developments or operational technol-ogy that forms a component of a capital project. Projects are typically delivered in a defined time period on a defined site. Projects have a clear start and finish. Projects may be restricted to one geographic site or cover a large geographical area, however, will be linked and not be geograph-ically diverse. A particular project may or may not be part of a program. Where a project is de-livered in multiple stages and potentially across varying time periods it is considered a 'complex project'. Refer to the definition for 'complex project'.
Project Information Model	PIM	Set of structured and unstructured information containers relating to the part of the lifecycle during which an asset is designed, constructed and commissioned. During the project, the project information model can be used to convey the design intent (sometimes called the design intent model) or the virtual representation of the asset to be constructed (sometimes called the virtual construction model).
Public financial corporations	PFC	Agencies classified by ABS that have one, or more, of the following functions: that of a central bank, the acceptance of demand, time or savings deposits or the authority to incur labilities and acquire financial assets in the market on their own account.
Public non-financial corporations	PNFC	Public sector entities comprising a range of government businesses providing major economic services. This includes state-owned corporations governed by the State Owned Corporations Act 1989. Commercial PNFCs receive most of their income from customers. Non-commercial PNFCs receive budget funding to meet policy objectives agreed with the NSW Government when income from customers is insufficient to meet operating expenses and/or capital expendi-ture.
Sensitive information		As defined in the Privacy Act 1988, is a subset of personal information and includes information about an individual's health, racial or ethnic origin, political opinions, religious beliefs, criminal record, or biometric templates. Sensitive data means information within the definition of 'sensi-tive information' as well as other types of data that are of a legally privileged, commercial-in-confidence, security classified, or environmental nature.
Shared data		Data made available to another agency, organisation or person under agreed conditions.

Smart community infrastructure		Community infrastructure with enhanced technological performance that is designed, operated and maintained to contribute to sustainable development and resilience of the community.
Spatially enabled digital twin		A digital twin integrated with spatial and positioning data, covering a defined geographic space above and below ground.
Stakeholders		People or organisations that can affect, be affected by, or perceive themselves to be affected by a decision or activity of the agency. For the purpose of this policy statement, stakeholders considered by the agency would include people and organisations both within and outside the NSW public sector.
State-owned corporations		PNFCs or public financial corporations (PFCs) which have been corporatised under the State Owned Corporations Act 1989.
Strategic Asset Management Plan	SAMP	Documentation of the activities required to establish, maintain and improve the agency's Asset Management Framework.
Transport for New South Wales	TfNSW	The lead transport and roads agency in New South Wales.
Uniclass 2015™		A UK classification system. Uniclass 2015™ is a classification scheme for the construction in-dustry. It is intended for organising library materials and for structuring product literature and project information. Uniclass 2015™ comprises tables, each of which represent a different class of construction information and deal with a different scale of information. Each table can be used as a standalone table for the classification of an information type. In addition, terms from differ-ent tables can be combined to classify complex subjects.
Victorian Digital Asset Strategy	VDAS	VDAS aims to improve the way infrastructure projects are defined, delivered and maintained in the Victorian Government.

Appendix C – Standards

Relevant Australian and international standards that can be used to support agency infrastructure data management in line with the IDMF include those in the following table:

Standard	Year	Title
AS/NZS 5478	2015	Recordkeeping Metadata Property Reference Set
AS 5488.1	2018	Classification of subsurface utility information (SUI), Part 1: Sub-surface utility information
AS 5488.2	2018	Classification of subsurface utility information, Part 2: Subsurface utility engineering
ISO 8000	2011	Data quality – Part 1: Overview
ISO 8000-2	2020	Data quality – Part 2: Vocabulary
ISO 12006-2	2015	Building construction - Organization of information about con-struction works - Part 2: Framework for classification of infor-mation
ISO 12006-3	2007	Building construction - Organization of information about con-struction works - Part 3: Framework for object-oriented infor-mation
AS ISO 15489.1	2017	Information and documentation - Records management - Con-cepts and principles
ISO 16739-1	2018	Industry Foundation Classes (IFC) for data sharing in the con-struction and facility management industries
AS/NZS ISO 19115.1	2015	Geographic information - Metadata – Fundamentals
AS ISO 19650-1	2019	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) - Information management using building information modelling - Part 1: Concepts and principles
AS ISO 19650-2	2019	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) - Information management using building information modelling - Part 2: Delivery phase of the assets
ISO/IEC 27000	2018	Information technology - Security techniques - Information se-curity management systems - Overview and vocabulary
AS ISO/IEC 27001	2015	Information technology - Security Techniques - Information secu-rity management systems - Requirements
AS ISO/IEC 27002	2015	Information technology - Security techniques - Code of prac-tice for information security controls
AS ISO/IEC 27003	2017	Information technology - Security techniques - Information security management systems - Guidance
AS ISO/IEC 27004	2018	Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation

ISO/IEC 27005	2018	Information technology - Security techniques - Information security risk management
AS ISO 29481.1	2018	Building information models - Information delivery manual - Meth-odology and format
AS ISO 29481.2	2018	Building information models - Information delivery manual - Inter-action framework
AS ISO 31000	2018	Risk management - Guidelines
ISO 37120	2018	Sustainable cities and communities - Indicators for city services and quality of life
ISO 37101	2016	Sustainable development in communities - Management system for sustainable development - Requirements with guidance for use
ISO 37122	2019	Sustainable cities and communities - Indicators for smart cities
ISO 37123	2019	Sustainable cities and communities - Indicators for resilient cities
ISO/IEC 38505-1	2017	Information technology - Governance of IT - Governance of data - Part 1: Application of ISO/IEC 38500 to the governance of data
ISO/IEC TR 38505-2	2018	Information technology - Governance of IT - Governance of data - Part 2: Implications of ISO/IEC 38505-1 for data man-agement
AS ISO 55000	2014	Asset management – Overview, principles and terminology
AS ISO 55001	2014	Asset management – Management Systems – Requirements
AS ISO 55002	2018	Guidelines for the application of ISO 55001

The NSW Spatial Collaboration Portal supports the following file types. For further information see https://enterprise.arcgis.com/en/portal/latest/use/supported-items.htm

360 VR Experience (.3vr)	AppBuilder Extension (URL)
AppBuilder widget package (.zip)—Only portal administrators can add this type of item.	Application (URL)
ArcGIS Desktop add-in (.esriaddin)	ArcGIS Explorer add-in (.eaz)
ArcGIS Explorer application configuration (. ncfg)	ArcGIS Explorer document (.nmf)
ArcGIS Explorer layer (.nmc)	ArcGIS for Windows Mobile package (.wmpk)
ArcGIS Pro add-in (.esriaddinx)	ArcGIS Pro configuration (.proconfigX)
ArcGlobe document (.3dd)	ArcMap document (.mxd)
ArcPad package (.zip)	ArcReader document (.pmf)
ArcScene document (.sxd)	CityEngine web scene (.3ws)
Code sample (.zip)	Comma-separated values (CSV) collection (.zip)
Comma-separated values (CSV) file (.csv)	Computer-Aided Design (CAD) drawing (.zip)
Deep learning package (.zip or .dlpk)	Desktop application (.zip)
Desktop application template (.zip)	Desktop style (.stylx)
Document link (URL to online document)	Feature service (URL)
File geodatabase (.zip)—If you publish a hosted feature layer, only feature classes (x,y features only), tables, attachments, and relationship classes are published.	Geocode service (URL)
Geodata service (URL)	GeoJSON file (.geojson or .json)
Geometry service (URL)	Geoprocessing package (.gpk)
Geoprocessing sample (.zip)	Geoprocessing service (URL)
Globe service (URL)	Image collection (.zip)
Image file (.jpg, .jpeg, .png, .tif, or .tiff)	Image service (URL)
Insights model (JSON)	Insights Theme (JSON)
iWork Keys (.zip)	iWork Numbers (.zip)
iWork Pages (.zip)	Keyhole markup language (KML) collection (. zip)
Keyhole markup language (KML) file (.kml or .kmz)	Layer (.lyrx)
Layer file (.lyr)	Layer package (.lpk or .lpkx)
Layout (.pagx)	Locator package (.gcpk)
Map package (.mpk or .mpkx)	Map service (URL)
Map service definition (MSD) (.msd)	Map template (.zip)
Microsoft Excel file (.xls or .xlsx)	Microsoft PowerPoint presentation (.ppt or .pptx)

Microsoft Visio drawing (.vsd)	Microsoft Word document (.doc or .docx)
Mobile application (URL)	Mobile basemap package (.bpk)
Mobile map package (.mmpk)	Mobile scene package (.mspk)
Network analysis service (URL)	Open Geospatial Consortium (OGC) Ge-oPackage (.gpkg)
Open Geospatial Consortium (OGC) Web Fea-ture Service (WFS) (URL)	Open Geospatial Consortium (OGC) Web Map Service (WMS) (URL)
Open Geospatial Consortium (OGC) Web Map Tile Service (WMTS) (URL)	Oriented imagery catalog (.oic)
Ortho Mapping Project (.json)	Ortho Mapping Template (.json)
Portable Document Format (PDF) (.pdf)	Pro map (.mapx)
Project package (.ppkx)	Project template (.aptx)
Raster function template (.rft.xml or .rft.json)	Relational database connection (URL)
Rule package (.rpk)	Scene layer package (.spk or .slpk)
Scene service (URL)	Service definition (SD) (.sd)
Shapefile (.zip)	Stream service (URL)
Survey123 add-in (.surveyaddin)	Tile package (.tpk or .tpkx)
Vector tile package (.vtpk)	Web mapping application (URL)
Workflow Manager service (URL)	Workflow Manager package (.wpk)

Appendix D – Information requirements checklists

The following Plain Language Questions (PLQs) can be used as a checklist to verify whether all bases have been covered from an infrastructure data management perspective. Note that the list is part of a living document and will be expanded over time.

Project Information Requirements

Strategic PIR:

- What is the proposed information management strategy?
- Is there sufficient information to produce Exchange Information Requirements?
- Are the exchange information requirements developed sufficiently to make decisions?
- What site information is to be provided?
- What format shall the information be delivered in?
- Have requirements for the delivery of asset information and data been identified?
- Is there appropriate management of information specifying: the security protection level or classification level of a project; security risk; and potential mitigation measures?
- Are there suitable measures in place for the protection of personal and commercial data and/or information?
- Have information / data exchange points at project stages been established (e.g. KPI's, asset data, PLQ validation)?
- Who will be able to use the data?
- Will all data be readily available to parties outside government – including parties working on government's behalf or third parties wanting to use information for private interests or shared public-private goals?
- Will there be a cost for accessing the data?
- Is there an opportunity for agencies to recoup some of the costs of data collection and its intellectual property?

Plan & Acquire IR:

- Do the supplier's proposals comply with the information requirements?
- What level of accuracy, detail, and information is required for concept and detail designs?
- Have the purposes of the 3D model(s) been defined?
- Are there any specific data requirements that need to be achieved?
- Are there any specific data standards and formats that can be followed?
- Do those standards and formats work for the agency?
- How will any client specific performance needs be met?
- What format shall the information be delivered in?
- How will special presentation needs be met (e.g. to stakeholders and approvers)?
- Is there an agreed information and data workflow?
- Is there a means of controlling distribution of models, documents and data, e.g. through a common data environment or other means?
- How will project information be used to support the infrastructure during the Operate and Maintain phase?
- Has the scope for operational and maintenance manuals for the infrastructure been defined?
- How accurate will the information be?

- What information do facilities managers need to manage the infrastructure and utilities?
- Have requirements for project information transfer into the AIM and integration into any enterprise asset management system been assessed?
- Have procedures for post-contract management of information been implemented?
- What Coordinate Reference System(s) shall the data be delivered and/or stored in?
- What spatial data transformation(s) are acceptable to that datum?

Asset Information Requirements

- How will data from the previous phases (design and construction) be verified and validated?
- Models, data and information including information provided for operation and maintenance are consistent with the organisational information requirements?
- Are measures being applied for the secure return, storage or destruction of asset information?
- Have procedures for post-contract management of information been implemented?
- Have appropriate measures been implemented to protect valuable, attractive and sensitive items, including all physical or information assets?
- Have requirements for project information transfer into the AIM and integration into any enterprise asset management system been assessed?
- Will the proposed information to be captured provide the level of data and information needed to support the information requirements of the organisation to underpin reporting, performance and capability analysis, and strategic planning aligned to outcomes?
- Is the data aligned to the organisation’s asset hierarchy and metadata standards?

NSW
GOVERNMENT