

Internet of Things (IoT) Policy Guidance

Document number:	Version number: 1.2
Date: Monday, March 08, 2021	

Contact details

Name: Office of the Secretary, Department of Customer Service
Email: iotproject@customerservice.nsw.gov.au

Table of Contents

CONSULTATION DRAFT:	1
Internet of Things (IoT) Policy Guidance	1
1. The Internet of Things in NSW	1
1.1 Introduction to IoT	1
1.1.1 What is IoT?	1
1.1.2 Why use IoT?	2
1.1.3 Applications of IoT	2
1.1.4 The IoT ecosystem	5
1.1.5 IoT and data	6
1.1.6 Trends in IoT	7
1.2 IoT in NSW Government	9
1.2.1 IoT opportunities for NSW Government	9
1.2.2 The current state of IoT in the NSW Government	9
1.2.3 Other relevant NSW Government policies and strategies	10
1.3 Purpose of the IoT Policy	11
1.3.1 Scope of the IoT Policy	11
1.3.2 Audience of the IoT Policy	12
1.3.3 How to use the IoT Policy	12
1.3.4 Case studies in the IoT Policy	12
1.3.5 How the IoT Policy relates to other NSW Government policies	12
1.3.6 Maintaining the IoT Policy	12
2. Project Scoping	13
2.1 Is IoT an appropriate tool to use?	14
2.2 Skills and expertise	21
2.2.1 Skills and expertise required to roll out an IoT-enabled project	21
2.2.2 Engaging with experts	22

3.	Project Planning	24
3.1	Project planning	25
3.1.1	What is project planning and why is it important?	25
3.1.2	Things to consider when planning an IoT-enabled project	25
3.1.3	Assigning roles, responsibilities and accountability	25
3.1.4	Planning for evaluation	26
3.1.5	Checklist of project planning considerations	26
3.1.6	Additional resources	28
4.	Stakeholder engagement	29
4.1.1	What is effective stakeholder engagement?	29
4.1.2	The importance of stakeholder engagement for IoT-enabled projects	29
4.1.3	How to effectively engage stakeholders	30
4.1.4	Additional resources	34
4.2	Data needs assessment	35
4.2.1	Understanding your desired business outcome	35
4.2.2	Engaging with stakeholders about data	36
4.2.3	Limitations in your operating environment	37
4.2.4	Improving data governance and management practices	37
4.2.5	Data requirements specification	38
4.2.6	Design and configuration for data collection	39
4.2.7	Data analytics	39
4.2.8	Data retention	40
4.2.9	Data storage	40
4.3	Risks and obligations	43
4.3.1	What is risk and compliance management?	43
4.3.2	How to manage risk and compliance	46
4.3.3	Ongoing communication and monitoring	47
4.3.4	Risk management standards	48
4.4	Privacy	49
4.4.1	The privacy regulatory landscape	49

4.4.2	Privacy and IoT	50
4.4.3	Privacy obligations around collecting and holding data	51
4.4.4	Best practice – Privacy by design	52
4.4.5	Privacy access requests and GIPA requests for information	56
4.4.6	Managing a data or privacy breach	57
4.4.7	Links for further information	57
4.5	Cyber Security	58
4.5.1	Securing IoT	58
4.5.2	NSW Cyber Security Policy requirements	58
4.5.3	Challenges in securing IoT	59
4.5.4	Vulnerabilities in consumer IoT devices	59
4.5.5	Cyber security guidance for organisations	62
4.6	Data obligations – open, shared and closed data	66
4.6.1	Open data	66
4.6.2	Shared data	66
4.6.3	Closed data	67
4.7	Technology for IoT	69
4.7.1	IoT architecture	69
4.7.2	Requirements in designing your architecture	69
4.7.3	The importance of interoperability in IoT solutions	71
4.7.4	‘What technology do I want or need?’ – Things to consider	72
4.8	Assurance	83
4.8.2	What assurance does my project need?	84
5.	Making the Case	87
5.1	Business case	88
5.1.1	What is a business case?	88
5.1.2	Why should a business case be prepared?	89
5.1.3	When should a business case be prepared?	89
5.1.4	How to prepare a business case	89
5.1.5	Additional resources	94

5.2	Cost-benefit analysis	94
5.2.1	What is a cost-benefit analysis?	94
5.2.2	How to conduct a cost-benefit analysis	94
5.2.3	Considering costs and benefits for IoT-enabled projects	95
6.	Procure	98
6.1	Procuring IoT solutions	99
6.1.1	Procuring IoT goods and services	99
6.1.2	Procurement landscape	99
6.1.3	Contacts for procurement	99
6.1.4	How do I procure?	100
6.1.5	What to do if the perfect solution does not exist	101
6.1.6	Designing specifications	101
6.1.7	Procurement risks	105
6.1.8	Disposal of assets	109
6.2	Data considerations for contracting	109
6.2.1	Data handling	109
6.2.2	Data ownership and rights	109
6.2.3	Data quality requirements	111
6.2.4	Data privacy and security	112
6.2.5	Application Programming Interfaces (APIs)	112
6.2.6	Cloud storage	112
6.2.7	Establishing clear responsibilities	113
6.3	Key contract terms for IoT solutions	114
7.	Set up	115
7.1	Change management	116
7.1.1	What is change management?	116
7.1.2	Why is change management necessary?	116
7.1.3	Managing change resulting from IoT-enabled projects	116
7.1.4	Managing ICT infrastructure change	117

7.1.5	Additional resources	118
7.2	Spatial data requirements	118
7.2.1	What is spatial data?	118
7.2.2	Introduction to the NSW Digital Twin	118
7.2.3	Recording IoT device position to meet spatial data requirements	119
7.2.4	GDA2020 and the Australian Terrestrial Reference Frame	120
7.2.5	Positioning standards	121
7.3	IoT deployment and configuration	123
7.3.1	Device deployment and configuration	123
7.3.2	Communicating about deployment	123
8.	Use and Maintain	124
8.1	Data analysis and use	125
8.1.1	The data analytics process	125
8.1.2	Using data for your business outcomes	130
8.2	Data sharing	131
8.2.1	Why and how to share data	131
8.2.2	Responding to requests for data sharing	132
8.3	Asset, device and data management	138
8.3.1	Asset management	138
8.3.2	Device maintenance	139
8.3.3	Data maintenance	140
9.	Assess	141
9.1	Evaluation	142
9.1.1	Why is evaluation important for IoT-enabled projects?	142
9.1.2	What to evaluate	142
9.1.3	How to evaluate IoT-enabled projects	143
9.1.4	Other assessment activities	146
9.1.5	Policy and resources	146
9.1.6	Why is auditing important for IoT-enabled projects?	148

9.1.7	Document management and record-keeping	148
9.1.8	The NSW Audit Office	148
10.	Appendices	149
	Appendix A – Pre-mortem exercise	149
	Appendix B – Privacy Collection Statement template	152
	Appendix C – Checklist for IoT solutions	153
	Appendix D – Key IoT wireless network options currently available in NSW	154
	Appendix E – The Five Safes	156
	Appendix F – NSW Government policy, framework or tool referenced in the IoT Policy	158
11.	Document Control	160
11.1	Document Approval	160
11.2	Document Version Control	160

1. The Internet of Things in NSW

Key takeaways from this module

- The Internet of Things (IoT) refers to an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.
- Although we have only seen the tip of the iceberg, IoT is already so pervasive that most people do not notice its presence and take for granted the services that it makes possible.
- Many projects may not be recognised as involving IoT, such as infrastructure projects like building a bridge or tunnel, but if they have sensors capturing data then they are IoT-enabled projects.
- The true value of IoT lies in the ability of organisations to use the information generated by IoT to gain insights for better decision-making and providing better services.
- No single IoT device or network can function alone as each component plays an interconnected role in the IoT ecosystem.
- Data needs to be considered at all stages of the project cycle if the benefits promised by IoT are to be achieved. This includes the security, collation and storage of data in a cohesive and consistent manner.
- The NSW Government is keenly focused on improving customer service, and IoT has potential applications for many services delivered by government.
- Effective deployment and use of IoT across the NSW Government requires a consistent approach, built on common understanding of opportunities, risks, obligations and best practice.
- This policy aims to give you a foundational level of IoT knowledge to enable you to have informed conversations with relevant experts.

1.1 Introduction to IoT

1.1.1 What is IoT?

The Internet of Things (IoT) refers to 'an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react' (21823.1:2020, Internet of things (IoT) - Interoperability for internet of things systems, Part 1: Framework, 2020)

This means 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 actuators, enabling these 'things' to share and exchange data to perform their functions more efficiently and effectively.

Being connected to the internet means that a 'thing' can:

- collect information and send it, or
- receive information and act on it, or
- do both.

Collecting, sending, receiving, and acting on information allows us to make more intelligent decisions with less human intervention. This can save time and money while also improving services.

IoT is likely to disrupt every aspect of our lives. In the coming decade IoT will be the driving force for innovation in all major economic sectors: health, education, agriculture, transportation, construction, manufacturing, utilities, entertainment. It will also create innovation opportunities between and across these traditional sectors.

The potential application of IoT is almost limitless. Although we have only seen the tip of the iceberg, IoT is already so pervasive that most people do not notice its presence and take for granted the services that it makes possible.

For example, Sydney commuters can access real-time information about their train journey on their smartphones thanks to complex IoT applications. They can access information like the train's location, projected arrival time at individual stations and the commuter capacity of each carriage. Behind the scenes, IoT sensors assist transport staff with tasks like track and train maintenance and performance management.

IoT is emerging to add value everywhere but there is often a low understanding of how it works and its implications. Rapid growth and the potential of technology is often accompanied by high risk and uncertainty.

For the purpose of this document, projects that involve IoT are referred to as IoT-enabled projects or solutions. While you may not consider your project to be an IoT-enabled project, it is important to recognise IoT elements in your project where they exist. Many

projects may not be defined as IoT-enabled, such as infrastructure projects like building a bridge or tunnel even though they use IoT sensors.

You may also find it useful to refer to the [glossary of IoT terms](#) published in the IoT European Large-Pilots Programme handbook. Note however that not all terms are relevant to the Australian context.

1.1.2 Why use IoT?

The application of IoT technologies has the potential to deliver significant benefits to government, industry and citizens, but its value is not guaranteed by its use alone. The true value of IoT lies in the ability of organisations to use the information generated by IoT to gain insights for better decision-making and providing better services.

The information, or 'data', collected through IoT sensors or smart devices can drive sustainability, liveability, workability, productivity improvements, economic efficiencies, and innovation. This data can also be used to drive other advanced technologies such as artificial intelligence (AI), augmented reality, digital twins and machine learning.

1.1.3 Applications of IoT

IoT solutions can be used for a wide variety of purposes. This is demonstrated in the diagram and in the case studies below.

Examples of applications of IoT



Using IoT for research

Case Study – NSW Department of Primary Industries using IoT for research

Through the **World-Class Food and Fibre Infrastructure Program**, the NSW Department of Primary Industries (DPI) is investing in IoT enabling infrastructure at its research sites. This creates the opportunity for DPI researchers to be more efficient in the delivery of research, and to solve problems through research that they previously could not solve. It also ensures that DPI remains in the top one percent of science institutions worldwide.

Since 2017 DPI has deployed low-power wide-area network (LPWAN) connectivity on nine of its research stations across NSW. This enabled DPI to trial established and emerging sensor technologies to see how they enhance decision-making on farms. The connectivity networks are open networks available for use by surrounding farms, universities and towns. Some of the applications being trialled include:

- solid state automatic weather stations
- salinity monitoring in fisheries research
- leaf wetness measurement as an indication of disease
- bore and water tank level monitoring
- beehive temperature, location tracking, and damage alerts
- irrigation channel level monitoring and pump operation alerts
- irrigation equipment GPS tracking
- greenhouse temperature and humidity monitoring
- low power GPS tracking of livestock.

The program commenced with a pilot to deploy IoT connectivity to six sites to test the technology and identify user needs for adoption. As at January 2020, 11 sites including Orange, Wagga Wagga, Tamworth and Griffith have IoT connectivity deployed, with the focus now shifting to DPI's remaining sites, and initiatives to accelerate capability, adoption and research impact.

The pilot has enabled DPI researchers to easily and remotely capture, store and analyse on-field data to make more efficient and data driven scientific decisions. This led to improved research outcomes and impact, and more effective farm management.

The pilots also seek to improve digital capability in primary industries by delivering training to local tech developers, universities, business suppliers and IT businesses, with a focus on climate adaptability and resilience.

DPI's IoT trials have delivered valuable insights around the complexity of the technology, gaps in technical skills of users and evidence of unclear or inconsistent value propositions for broad-scale primary industries adoption.

Using IoT for Green Infrastructure

Green infrastructure is the network of green spaces, natural and semi-natural systems in place to support a good quality of life for communities in the urban environment. Such infrastructure includes waterways, bushland, tree canopy, green ground cover, parks and open spaces.

IoT can be used in green infrastructure to:

- capture data on localised temperature, humidity and air quality and visibility to support proactive measures to protect people's health and safety while enjoying green open spaces.
- aggregate and analyse environmental data from IoT devices to provide real time insights on the environment to drive biodiversity and sustainability outcomes. Examples include tree health, soil moisture, water and air pollution levels, urban heat, threatened species monitoring and irrigation management.
- provide water monitoring IoT solutions that support water asset maintenance, contributing to water efficiency and waterway health.

Case Study - Wollondilly Shire Council's using IoT for a better community experience

Wollondilly Shire Council sponsored a smart parks project from the 2019 Digital Western Parkland City Pitchfest. IoT technology was trialled to improve the community's experience of public open space and operational efficiencies for council maintenance staff.

At the time, the Shire had poor mobile and internet connectivity, making it challenging to monitor and maintain council owned public open space.

Telopea Park in Buxton was chosen as the trial site. Technologies trialled included 'smart pole' infrastructure to support Wi-Fi, LoRaWAN and mobile connectivity, and IoT sensors to monitor parking, waste, and BBQ and amenities block usage.

During the height of COVID-19 restrictions, Wollondilly Shire Council used the IoT network and sensors to monitor park usage to ensure compliance with public social distancing and self-isolation requirements.

Case Study - Liverpool City Council using IoT for environmental care

As part of the 2019 Digital Western Parkland City Pitchfest, Liverpool City Council and the Department of Planning, Industry and Environment co-delivered a digital tree register and tree monitoring project in the Casula Parklands.

IoT sensors were placed in the ground next to 10 trees to monitor soil temperature and humidity. The data captured from these sensors was directed to a dashboard where it was visualised as a traffic light system to indicate when a tree needed watering, accompanied by weather forecasting that included predicted rainfall.

After the success of the trial, Liverpool City Council is now looking to scale the solution to monitor 245 trees as part of the Liverpool Urban Forest Strategy. The expansion will create individual tree profiles on an open platform to encourage tree care from the community.

1.1.4 The IoT ecosystem

It is easy to focus on the physical device when thinking about IoT. However, this is just one element of the IoT ecosystem. Like the human body, no single IoT device or network can function alone as each component plays an interconnected role within the IoT ecosystem. Broadly, an IoT ecosystem includes:

Things: Machines, equipment, devices and other physical assets to which IoT hardware is applied, allowing them to sense and affect the surrounding physical environment, receive and transfer data and interact with control units and other enabled things.

IoT hardware: Sensors, actuators, instruments and other components that capture and relay contextual information and real-world data and enable the 'thing' to communicate with its environment.

IoT backbone: The capture and storage of the raw data received from the connected 'things', and the processing, storage (cloud, servers, data centres) and management of this data.

Communication and network: network hardware, software, protocols and services that connect IoT hardware to the internet, whether that is:

- Backhaul connectivity: long-haul communications; GPS, cable, LPWANs, cellular
- Local connectivity: short-range and machine-to-machine communications; WLAN, mesh networks, Bluetooth, Wi-Fi
- IoT gateways: intermediaries between the sensors/actuators and the cloud to process the collected data locally before sending it to the cloud.

See [Appendix D](#) for a table of key wireless network options available in NSW.



Visualisation and communication: Data visualisation is about the visual representation of data as a means of communication. Data needs to be delivered to the organisation in a meaningful way to support decision making. Examples include dashboards, push notifications, interactive public displays, enhanced 3D spatial platforms and digital twins etc.



Solution services: Services that integrate the components of the system into the business and physical environment, including the development of solutions, platforms, devices, and vertical applications, and system integration, testing, managed services and support.



IoT platforms: Software that turns the raw data into a common language and connects the other elements of the IoT ecosystem to each other. Interoperability is crucial when choosing your IoT platform. See [Chapter 3.8 Technology for IoT](#) for information on interoperability.



Identity and security (platforms): Software and hardware that enable identity authentication and management, cyber security and end-point protection.



Data transfer management and processing applications: Software that facilitates transfer, manage and process data, comprising of middleware (e.g. Service Bus), backend data processing (e.g. database and decision units), and frontend user and Business-to-Business (B2B) interfaces. These applications provide intelligence and insights generated from data such as:

- Analytics: Aggregate, analyse and package data to extract insights. This includes big data analytics that enables applications to aggregate and acts on large amounts of data generated by devices. Aggregated data can drive innovation, research, and marketing, as well as optimise the services that generated it.
- Enterprise and consumer apps: Applications that leverage IoT data and algorithms to solve problems and address needs. An example is the [train tracking application in Section 1.1.1 What is IoT?](#)

For further information on the IoT ecosystem, see the [Australian Computer Society \(ACS\) Report prepared by PwC, Australia's IoT Opportunity: Driving Future Growth \(2018\)](#).

Refer to [the IoTAA: IOT Reference Framework](#) for identifying and positioning elements of the IoT ecosystem. See also the [National Code of Practice](#) which is a voluntary set of measures the Australian Government recommends for industry as the minimum standard for IoT devices.

1.1.5 IoT and data

Data is a critical element of IoT and a core output of any IoT-enabled project. In the IoT ecosystem, observations made by connected devices or sensors are transmitted, stored, processed and analysed as data. Data needs to be considered at all stages of the project

cycle if the benefits promised by IoT are to be achieved. Individual sensors may be cheap, but data is not.

Data in IoT initiatives can mean a range of things. Data can be text, binary, structured, freeform, data processed into rules and policies or trained machine learning models. Data can also flow in a range of ways. For example, sensors can send their data to a central cloud server for analysis and storage, or data can flow from peer to peer like a sensor supplying data to an actuator.

1.1.6 Trends in IoT

The number of deployed IoT devices in the world is expected to grow exponentially. The [International Data Corporation \(IDC\)](#) estimates there will be 41.6 billion connected IoT devices by 2025 worldwide compared to an estimated 14.2 billion connected things in 2019. The IDC also estimates that worldwide technology spending on IoT will reach US\$1.2 trillion in 2022 compared to US\$745 billion in 2019. For 2019 it is predicted that the largest IoT market will be discrete manufacturing (US\$119 billion), followed by consumer retail (US\$108 billion), process manufacturing (US\$78 billion), transport (US\$71 billion) and utilities (US\$61 billion).

Domestically, the [Australian Computer Society \(ACS\) Report prepared by PwC, Australia's IoT Opportunity: Driving Future Growth \(2018\)](#) found that IoT has potential annual benefits for Australia of \$194-308 billion over 8 to 18 years. This translates to approximately two percent per annum in productivity improvements in the construction, manufacturing, health, food/agriculture, and mining sectors.

According to [Gartner](#), the top technology trend for IoT is an increase in artificial intelligence (AI) being applied to data and information that is collected through IoT devices. IoT service providers are expected to invest heavily in AI in the coming years. It is widely agreed that AI will increasingly drive IoT development and deployment, as the number and complexity of IoT systems, and the data collected and analysed, exceed human capability.

Gartner predicts the monetisation of data becoming a strategic business asset and that it will become an essential part of many IoT ecosystems by 2030. As IoT matures and becomes more widely deployed, social, ethical and legal issues will become more important. An IoT governance framework that ensures appropriate behaviour in the creation, storage, use and deletion of information related to IoT-enabled projects in the private sector will also become more vital.

Sensors and technology will continue to evolve and innovate. By 2023 it is expected that new special-purpose chips will be developed to operate on high-performance networks with lower power consumption. These will support new functions such as data analytics integrated with sensors.

IoT architecture trends will continue to shift from centralised and cloud architecture to edge architecture, and then towards unstructured and connected dynamic mesh architecture enabling more flexible, intelligent and responsive IoT systems.

The below diagram illustrates the trends outlined in this section.

Predicted trends in IoT



41.6 billion

connected IoT devices by 2025

US\$1.2 trillion

worldwide technology spending on IoT in 2022



A\$194-308 billion

Potential annual benefits of IoT in Australia over a period of 8-18 years

2% growth

per annum in productivity improvements



Top IoT technology trends



Artificial Intelligence (AI)



Monetisation of data



Specialised chips for higher device performance on lower consumption by 2023



Shift from **centralised** and **cloud** architecture, to **edge** architecture, to **mesh architecture**



Social, ethical and **legal** issues, and **governance** framework to monitor IoT in private sector

1.2 IoT in NSW Government

New South Wales will embrace IoT to be the most innovative, integrated, intuitive Smart State in Australia. We will lead the way in employing IoT to deliver better, more accurate and evidence-based services which improve the lives of citizens.

1.2.1 IoT opportunities for NSW Government

The NSW Government is keenly focused on improving customer service. IoT has potential applications for many services delivered by the government which can help agencies to:

- collect and analyse data on citizen's needs, priorities and interactions with government, contributing to evidence-based policy and service delivery
- access more accurate real-time data, which can, for example, enable the delivery of on-demand services tailored to individual needs
- model changes to policy and services in a safe environment to better understand the impacts of decisions prior to implementation
- integrate and redesign services in ways that save citizens time, increase productivity and improve the customer experience.

The NSW Government has an obligation to its citizens to boldly experiment, collaborate and learn. Through experimentation and innovation, we deliver better services more efficiently. Through collaboration, we break down siloes to deliver seamless services for our customers. When we share what we learn, we lift capability across the sector and community.

While IoT presents many exciting opportunities for the government to better serve its customers, these opportunities are not without risk. The NSW Government is committed to the safe adoption of IoT, which means protecting privacy, minimising risks and ensuring citizens' security.

1.2.2 The current state of IoT in the NSW Government

The NSW Government is regularly ranked as the most digital-ready government in Australia. However, taking advantage of opportunities presented by IoT requires upskilling across the sector to ensure we innovate efficiently, effectively and safely.

There are small passionate teams in various agencies undertaking IoT-enabled projects. Some of these teams are very experienced, whilst others learn as they go. This means that often the projects are ad hoc, have a narrow focus on operational efficiency rather than a strategic opportunity, and experiences and learnings are not shared. Projects are developed in silos, so they aren't designed for interoperability and cross-silo benefits.

There is a growing interest in taking advantage of the efficiency gains and decision-making enhancements presented by IoT. This excitement is tempered by a lack of confidence in planning and executing an IoT-enabled project in a way that will maximise benefits and

keep risks within tolerance levels. This policy provides guidance to address these concerns and risks.

1.2.3 Other relevant NSW Government policies and strategies

The NSW Government has suite of existing policies and strategies that support IoT.

Smart Places Strategy

Smart Places integrate technologies into the built environment to capture and convey data and insights. This includes using IoT devices to collect and analyse data about an asset or local environment. The data can help NSW Government to make evidence-based decisions to improve infrastructure, services and liveability for the NSW community.

The [Smart Places Strategy](#) sets out the NSW Government's vision for Smart Places, in particular how it will work collaboratively with local government, Australian Government and private sector partners to harness the power of digital technologies and realised the substantial benefits being delivered by technological change.

Smart Infrastructure Policy

The [Smart Infrastructure Policy](#) sets the minimum requirements for smart technology (including IoT) to be embedded in all new and upgraded infrastructure from 2020. The Smart Infrastructure Policy applies to all new NSW Government capital and ICT projects subject to the Investor Assurance Framework (IIAF) and the ICT Assurance Framework.

Artificial Intelligence Strategy and User Guide

[Artificial Intelligence](#), or AI, is intelligent technology, programs and the use of advanced computing algorithms that can augment decision making by identifying meaningful patterns in data. AI in this context should aim to help the NSW Government free up our workforce for critical and frontline tasks, cut costs and enable us to deliver better, more targeted services.

The [NSW Government AI Policy and User Guide](#) provides clear guidance on the safe use of AI, finding the balance between opportunity and risk, while putting in place those protections that would apply for any service delivery solution. A new body, the AI Advisory Committee, chaired by the NSW Government Chief Data Scientist, can assist agencies with AI project plans to ensure consistency with the AI Ethics Policy.

Infrastructure Data Management Framework

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.

Spatial Digital Twin

The [NSW Spatial Digital Twin](#) is upgrading the state's Foundation Spatial Data Framework (FSDF) from a two-dimensional map to a four-dimensional model (3D + time). That is, a full three-dimensional model of the state's physical environment, capable of recording past conditions and visualising future scenarios to create a digital real-world model of our cities and communities which will facilitate better planning, design and modelling for NSW's future needs. The NSW Spatial Digital Twin will provide the platform upon which government, developers and residents are able to visualise, plan, develop and assess infrastructure (such as transport links), new community facilities, public spaces, and homes. For further info see [Spatial data requirements](#)

1.3 Purpose of the IoT Policy

IoT is a new, complex and rapidly changing environment. There are pockets of the NSW Government with experience in designing and rolling out IoT solutions however, the sector's maturity is generally low.

Effective deployment and use of IoT across the NSW Government requires a consistent approach built on a common understanding of the opportunities, risks, obligations and best practice. The potential of IoT to improve customer service across all categories of goods, services and infrastructure will only be realised through greater investment and experimentation.

This policy has been designed to:

- demystify IoT
- encourage innovation with IoT solutions
- build understanding and capability across the sector
- provide practical guidance for those responsible for delivering IoT-enabled solutions.

1.3.1 Scope of the IoT Policy

The IoT Policy provides:

- practical guidance to help organisations design, plan and implement IoT solutions
- advice on standards and obligations where available and practical
- tools and templates to help effectively manage an IoT-enabled project
- guidance on where and how to source additional advice if required.

The diversity of applications – and potential applications – of IoT across the NSW Government makes it impossible to provide prescriptive guidance suitable for every IoT solution. Rather, this policy provides IoT solution-agnostic advice and recommendations for where to find additional information.

Navigating the successful development and rollout of an IoT-enabled project requires a wealth of diverse technical knowledge which cannot be conveyed in a single policy. This

policy aims to give you a foundational level of IoT knowledge to enable you to have informed conversations with relevant experts.

1.3.2 Audience of the IoT Policy

The primary audience for the IoT Policy is NSW Government agencies that are planning or currently implementing IoT solutions, or that are interested in learning more about the applications of IoT.

Local government will also find the IoT Policy useful. While some of the obligations outlined in the IoT Policy may not apply to organisations outside of the NSW Government, most of the advice in the policy is relevant to local government.

1.3.3 How to use the IoT Policy

This policy is divided into eight standalone modules which contain chapters. Each module relates to a step of the reader's 'IoT journey' in implementing an IoT-enabled project.

At the beginning of each module, you will find a checklist of key takeaways (for modules 1 and 2) or best practice considerations (for modules 3 to 8).

You can read the policy in its entirety or select the module relevant to the step in your IoT journey.

1.3.4 Case studies in the IoT Policy

Case studies are used throughout this policy to illustrate the concepts and uses of IoT.

1.3.5 How the IoT Policy relates to other NSW Government policies

This policy refers to other NSW Government policies, frameworks, and tools that provide context and information relevant to IoT in NSW. They are listed in the table at Appendix F.

This policy does not override existing agency policies and standards where they exist. It is important that you contact the subject matter experts in your organisation for guidance on any organisation-specific policies and standards.

1.3.6 Maintaining the IoT Policy

The IoT ecosystem is rapidly evolving. Associated policies should be flexible and adaptable enough to accommodate changes.

To ensure its usefulness, this policy will be regularly updated as technologies change, opportunities and risks are better understood, standards develop, and IoT maturity across NSW Government grows.

2. Project Scoping

Key takeaways from this module

- It is important to consider IoT early in your project. It can be more challenging and costly to incorporate IoT as your project progresses (rather than planning for it upfront).
- Things to contemplate when considering the use of IoT include your project intent, time, location, resources, systems and processes, and risks.
- When thinking about resources and skills, you need to consider the whole of life resourcing needs for your IoT-enabled project.
- The specific skillset required for your IoT-enabled project will depend on your knowledge and experience, the type of IoT solution you are implementing, what you intend to do with the data collected and whether devices exist that meet your needs.

2.1 Is IoT an appropriate tool to use?

This chapter will help you determine whether IoT is an appropriate tool to achieve your intended outcome.

It is best to consider the suitability of IoT early on in your project. It can be more challenging and costly to incorporate IoT as your project progresses rather than planning for it upfront.

The following table contains key things to consider before committing to the use of IoT.

Considerations when determining if IoT is an appropriate tool for your project

Consideration	Questions to ask	Follow on questions and explanation
Project intent	Does IoT allow you to meet your intended goal, solve your problem and/or produce a benefit?	<p>An IoT solution collects and communicates data and information and can be used to inform decisions and actions. Consider the outcome you want to achieve, the nature of the problem you seek to solve or the system or service you seek to improve.</p> <p>Can IoT help solve the problem you are trying to address? It is easy to get lost in the multitude of applications that IoT presents and be overwhelmed by the IoT hype. In some instances, project managers are asked to design and implement an IoT-enabled project without proper consideration of what role IoT can play in solving the problem. IoT is not suitable for all projects; it is important to clarify your problem statement and determine if an IoT solution will help you solve it.</p>

Consideration	Questions to ask	Follow on questions and explanation
		<p>Start to think about data – is data or information necessary to help achieve the desired change? If yes, what data will be needed? How will the data be used/analysed? What is the most effective way of collecting the data?</p>
	<p>Are there other solutions that will achieve the same outcome?</p>	<p>What alternative solutions exist that could achieve the outcome you are looking for? If there is an alternative, is IoT the better option? Does it deliver better value for money and/or superior benefits?</p>
	<p>Can IoT enable you to use other forms of technological solutions to improve services?</p>	<p>IoT itself can be a solution but it is also an enabler for other technologies (i.e. digital twins, artificial intelligence (AI), machine learning or augmented reality). Data collected by your IoT solution may also facilitate your agency's use of other data-intensive technologies.</p> <p>Data collected from other projects or external sources may also provide valuable sources of information. You may not need to collect new data for everything needed on the project.</p>
<p>Time</p>	<p>Do you need to collect data as a 'one-off' or periodically, frequently or even continuously for a length of time?</p>	<p>One of the biggest benefits of IoT solutions is the ability to collect information on a frequent basis so that the cost per collection is lower. If you only require data to be collected</p>

Consideration	Questions to ask	Follow on questions and explanation
		<p>infrequently, consider if there is a positive cost-benefit to deploying an IoT solution compared to collecting data manually or using another method.</p> <p>In some cases, real-time or near real-time data can add new operational insights previously impossible prior to the emergence of IoT technologies.</p>
	Will you save time by implementing an IoT solution?	Does your current process involve many employee hours travelling to locations to collect information in person? A significant benefit of installing an IoT solution is that it can remove the need for employees to collect and communicate information manually.
	Can your organisation commit to IoT in the long term?	IoT is a long-term commitment and should not be expected to succeed with a set and forget approach. Setting up and maintaining an IoT solution is a significant investment of time and money, and once installed can be in place for many years during which there will be technology changes.
	Is now the right time to commit to IoT?	Do you have the time to commit to implementing a new process with new technologies? Do you have the resources?

Consideration	Questions to ask	Follow on questions and explanation
		<p>Do you have the buy-in from senior stakeholders?</p> <p>The IoT market and associated technologies are rapidly maturing, costs continue to decline, standards are being considered and adopted, and the process of implementing IoT solutions is becoming easier. If now is not the right time, the situation may soon change.</p>
Location	<p>Are there any environmental factors that might interfere with the IoT?</p>	<p>Thinking about the environment in which your IoT devices will be placed, is there anything that could impact your ability to install the sensors or their ability to function? Is it rural or far from any network connection? Is it in a coastal area that may be affected by the tide? Is it in the middle of the city on pylons that you cannot access? Is it in a fire-prone area? Is it underground (in which case there may be signal loss)?</p>
	<p>Will you be able to connect to a network?</p>	<p>IoT devices work by transmitting information that is collected by the device to a hub that then responds to the information. Devices need to be connected to a network to be able to do so. This can be a challenge in areas where no network access currently exists or signal strength is weak, and you may need to install additional technical devices to access a network. This may be the case, for</p>

Consideration	Questions to ask	Follow on questions and explanation
		example, in some rural and remote areas or underground.
	Do you own or have access to the infrastructure/land where the IoT solution will be installed?	Do you have the authority/access to the right infrastructure (e.g. buildings, telegraph poles, networks) and land that is necessary to implement the IoT solution?
Resources	Do you have access to the technical expertise that may be required to set up and run an IoT solution?	Depending on your project needs, the perfect IoT solution may or may not exist. If it does not, do you have access to the technical expertise required to build your own IoT solution or work with a service provider to build a solution for you?
	Who will maintain the IoT devices and system?	Do you have adequate human resources to maintain the IoT solution and associated data? If a device needs maintenance, will you be able to respond? Who will maintain the datasets the IoT solution produces?
	Do you have the budget for the whole-of-life requirements for IoT?	IoT-enabled projects do not end once the sensors have been purchased and installed. Devices require ongoing maintenance, as does data and information that is collected.
Systems and processes	How will your IoT solution interact with or impact on current and future systems and processes?	An IoT solution is not a standalone process nor a product. It will either become a part of your current systems or it will interact with them. This includes ICT, organisational,

Consideration	Questions to ask	Follow on questions and explanation
		<p>operational and financial systems and processes.</p> <p>It is also important to plan for the rapid evolution of technology. This means IoT solutions should be as technology agnostic as possible to minimise the need for costly re-integrations and re-writes when new technologies require re-fit of old technology</p>
	<p>Can you integrate the new IoT system into your existing system?</p>	<p>Will there be any issues with an IoT solution being implemented and integrated into your current systems?</p>
	<p>Is human intervention still required in the process?</p>	<p>If you install IoT devices, will you still require staff to attend the location for information collecting or other purposes? Think about whether installing an IoT solution makes a positive impact on the process and reduces the time required for employees to deliver the outcome.</p>
Risk	<p>How critical is the system that you are planning on using IoT for?</p>	<p>If there is a network interruption or repairs are needed for the IoT device, will the disruption cause serious negative consequences? Will it cause other systems to fail? If the system and information are hacked, will critical information be at risk?</p>
	<p>How sensitive is the data you need to collect?</p>	<p>Will device encryption be enough to protect the data you are collecting, or are you</p>

Consideration	Questions to ask	Follow on questions and explanation
		working in a sensitive area where certain information should not be collected and transmitted by IoT devices?
	Do you know how to make decisions about how to appropriately share your data and protect any personal or sensitive information?	Data gathered for a project may contain sensitive information. You need to know how to preserve privacy and trust while sharing data with others.

Case Study – Sydney Water’s digital metering trial

Sydney Water is trialling digital metering to test the technical reliability, connectivity, and handling of different digital metering solutions for non-mission critical monitoring activities.

Sydney Water explored various technologies in the first phase of the trial:

- retrofits for mechanical meters
- digital/smart meters
- Smart Meters with integrated pressure and temperature sensors
- 80 digital meters fitted to residential and commercial sites.

Sydney Water deployed around 1500 sensors into the field, including sewer level sensors in high-risk areas and digital flow meters on customer properties. The trials showed some early benefits; for example, the system detected a number of blockages in sewers which Sydney Water crews could clear before customers or the environment were impacted.

As at June 2020, the next phase of the trial will deploy ‘thousands’ more of the sensors to gather more robust insights on how digital metering can support Sydney Water’s objectives of general water consumption reduction, asset investment deferral and reduction of system losses and network leakage.

2.2 Skills and expertise

This chapter will help you consider what skills and expertise your project team may need at different points in the lifecycle of your IoT-enabled project. It provides advice on ways to address any gaps.

2.2.1 Skills and expertise required to roll out an IoT-enabled project

When thinking about resources and skills you need to consider whole of life resourcing needs. Whole of life resources include the time and labour required to plan for, deliver, maintain and assess your project.

The specific skillset required for your project will depend on your knowledge and experience, the type of IoT solution you are implementing, what you intend to do with the data collected, and whether devices exist that meet your needs.

Implementing your project may require a broad spectrum of skills in areas including, but not limited to:

- *Data*: To assist with determining your data requirements and ensure they are met. The collection, processing, analysis, presentation and interpretation of IoT data and insights requires a range of specialist skills. Key roles include:
 - Business domain experts
 - Data architects, engineers, analysts, scientists, visualisers, and storytellers

- *Cyber security*: To verify that your IoT solution is safe and secure
- *Privacy*: To help ensure that your IoT solution is compliant with privacy legislation
- *Legal*: To check that all legislative obligations are met
- *Procurement*: To assist with procuring the elements of the IoT ecosystem
- *Finance*: To assist with cost-benefit analysis, budgeting, economic evaluation and audit
- *Evaluation and audit*: To conduct an independent evaluation and/or audit, or to assist with doing so
- *Field installation and maintenance staff*: To install and maintain sensors and/or network equipment
- *Technology skills*: Obtaining specialist technology input will ensure that necessary infrastructure and tools are in place to support your project requirements, such as data modelling and processing, secure information transmission and storage, and integration and analytics. Specialist skills are useful for:
 - Hardware interfacing: to interface sensors and transmitters
 - IP networking: to set up the network used to communicate information
 - UI/UX design: to design the interfaces between the IoT device and the user
 - Reference architecture: to set up the architecture for the IoT solution and ensure that your IoT solution fits within the broader organisational architecture
 - Machine learning and artificial intelligence: to work with the data received
 - System configuration: to program and configure IoT devices at all levels of the ecosystem.



Tip: IoT experts exist and may have a combination of the above skills. If you have the resources, you may choose to engage a specialist consultant who has the skills and experience you require. Check that they have the experience (preferably in your subject area), good references and a sound reputation.

2.2.2 Engaging with experts

It is unlikely you will require all the skills listed in this chapter throughout your entire project. If you do not have the relevant skills within your team, you may wish to engage experts.

Look within your organisation for internal expertise or look more broadly across the NSW Government for expertise. Engaging with experts should form part of your stakeholder engagement strategy (see [Chapter 3.2 Stakeholder engagement](#)).

The NSW Department of Customer Service has a [Cyber Security team](#) that can provide advice and guidance on managing the cyber security elements of your IoT system or solution. Similarly, the [Data and Analytics Centre Program and Practice team](#) can provide general guidance and advice on managing your IoT-generated data. If your organisation has a data governance committee or group, notify them of your project. If not, consider establishing one to ensure effective decision-making about data issues.

Another way to engage with experts is to join a NSW Government Community of Practice (ComPrac). [Membership](#) is free and open to all NSW Government employees, and it provides access to free resources, events and networking. ComPracs exist for areas including procurement, finance, change, customer experience (CX), policy, ICT, records management, and commissioning and contestability.

You can also reach out to other organisations that have experience with IoT to learn from their successes and challenges, within NSW and in other states and countries. There may be opportunities to leverage the research and accumulated knowledge of academia through formal partnerships or informal advice to supplement your team's skills and expertise.

Industry associations and other organisations are also a valuable source of knowledge. Organisations in the IoT space include:

- [Internet of Things Alliance Australia \(IoTAA\)](#)
- [OpenCities](#)
- [Communications Alliance](#)
- [Design Futures Council](#)
- [Australian Smart Communities Association](#)
- [Standards Australia](#).

3. Project Planning

Best practice considerations at this stage in a project

- Are there governance processes, including responsibilities, accountabilities and decision-making delegations appropriate to the stage of the project to manage, monitor and report on project progress and benefits realisation?
- Do you have access to the resources required with the appropriate skills and experience (such as commissioning, transitioning, operations, cyber, data, privacy etc)?
- What are the long-term broader asset network and service integration requirements, and have they been articulated and appropriately captured through the option assessment process?
- Has the impact of the proposed project on staff, other people (including the community), existing infrastructure and processes been evaluated and documented?
- Do you understand how your current network will interact with the proposed solution? Have you considered the costs?
- Are there plans for stakeholder management, engagement and communication that have considered the influence of, and impact on, each stakeholder or stakeholder group?
- Have you identified current, anticipated and emerging risks and issues, and have you recorded them in a risk register that is up to date and monitored? Does this include a risk management plan that outlines ownership for risk mitigation?
- What are the existing or high probability issues that could diminish the delivery of the project over time and how will they be mitigated?
- Are there major risks to the project going live on-time, on-budget and to agreed scope? If yes, are these risks being managed?
- Have key stakeholders been consulted in developing key project documents including the risk management plan? Do the risk owners understand their responsibilities, in addition to the risk escalation process?
- Can the organisation implement any new services under the project and maintain existing services?

3.1 Project planning

3.1.1 What is project planning and why is it important?

A project plan (sometimes called an implementation plan) outlines how you will deliver your project. Developing a plan and understanding how each element of your IoT-enabled project will be delivered will help mitigate risks that can undermine it.

Given the newness and complexity of IoT-enabled projects and the number of factors that need to be considered to deliver a successful project, it is important to plan upfront.

3.1.2 Things to consider when planning an IoT-enabled project

You need to understand and consider your organisation's goals, strategic directions and your business problem prior to starting your IoT-enabled project. It is worthwhile exploring if your project feeds into a larger portfolio or program of work, such as to 'make your city smarter'. This will help you to achieve alignment between your project and existing priorities.

Take time to consider the needs of your users and customers. Having customers at the centre of your IoT-enabled project can provide a focus for prioritising issues and solutions and ensuring that your project addresses what it is intended to ensure it is successful.

While there is no whole of government project planning policy, organisations may have their own project planning guidelines and/or a Project Management Office to assist with project planning and project management.

3.1.3 Assigning roles, responsibilities and accountability

Projects require adequate oversight and management to ensure that plans are followed, risks are minimised, decisions made remain relevant and benefits are maximised. The multifaceted nature of IoT means it is essential that roles and responsibilities are assigned and understood for each aspect of your project, including data, cybersecurity, privacy, hardware, software applications, and system architecture.

a) Responsibility for data

You need to make certain that clear responsibilities are allocated for IoT data ownership and management. Your organisation's data governance frameworks should identify who has responsibility for your IoT data and who is responsible for giving permission for open data release or data sharing. Data sharing agreements should specify data rights, including whether ownership of the data will be transferred to the third party.

Even under service arrangements, NSW Government agencies are the custodian holding overall accountability and responsibility for their data. A NSW Government agency may delegate its responsibility for the day-to-day creation and management of data to another organisation, but it will continue to have overarching responsibility for the integrity and accountability of its data. These responsibilities are usually delegated to Secretaries or agency heads under different NSW legislation. This means that each NSW Government

agency must ensure that any legal risks are managed and controlled, including ownership and sovereignty issues.

In addition, all data and information assets that are products of NSW public sector bodies fall under the [State Records Act 1998 \(NSW\)](#). Under the Act, custodians are responsible for the creation, management, protection and maintenance of their datasets, even when these management responsibilities have been delegated to another agency.

See [Chapter 5.2 Data considerations for contracting](#) for more information on contractual arrangements around data ownership and responsibilities.

3.1.4 Planning for evaluation

Evaluation planning should start when the project is being designed and planned. Much of the planning for evaluation can be completed before the project has started to be implemented.

Planning for evaluation means that you can set a baseline against which you evaluate the results of your project. You will also know what data and information to collect during the project to support your evaluation. Integrating evaluation with the project cycle supports a stronger, more effective evaluation, and helps to identify outcome measures and KPIs for your business case.

See the [Evaluation Toolkit](#) for assistance on developing evaluation plans, and speak to your organisation's Evaluation team. Further information on evaluation can be found in [Chapter 8.1 Evaluation](#).

The evaluation process across the project or program cycle



3.1.5 Checklist of project planning considerations

Below is a checklist of considerations you can use in developing your project plan:

Skills and expertise (see [Chapter 2.2 Skills and expertise](#))

- I have access within my organisation to the skills I need to deliver my project
- I have access to the necessary people and resources external to my organisation

Roles, responsibilities and accountability (see [Chapter 3.1 Project planning](#))

- I have clearly assigned roles and responsibilities for all elements of my project, including for the data that will be generated

Data needs assessment and data obligations (see [Chapter 3.3 Data needs assessment](#) and [Chapter 3.7 Data obligations](#))

- I understand how the data developed through my project will be collected, transmitted, stored, structured, processed, analysed, used and released
- I know who owns the data that is to be collected
- I have developed metadata requirements
- I am aware of any data-related limitations in my operating environment and how they may impact the use of the IoT-generated data or its integration with work processes
- I understand what open data standards are applicable to my project and what data that I collect should be made open
- I understand the [State Records Act 1998 \(NSW\)](#) requirements I must comply with

Risk (see [Chapter 3.4 Risks and Obligations](#))

- I understand what risks my project may be exposed to
- I have a plan to mitigate identified risks

Privacy (see [Chapter 3.5 Privacy](#))

- I understand my organisation's privacy obligations, identified key privacy risks and identified appropriate treatments for those risks

Cyber security (see [Chapter 3.6 Cyber Security](#))

- I understand the cyber security requirements that the project will need to consider and address

Technology for IoT (see [Chapter 3.8 Technology for IoT](#))

- I know what sort of devices I need, and I know if they already exist or if I need to custom build them
- I know what IoT architecture options exist and which one is best for my project

- I know what products or systems exist (now and in the future) that the IoT solution will need to be interoperable with
- I understand the network technology that exists in the areas I need to deploy the technology, and the best network to use for my needs now and into the future (e.g. in five years)

Stakeholder engagement (see [Chapter 3.2 Stakeholder engagement](#))

- I have identified the various parties that will be impacted by the project, including citizens
- I have a plan to engage with internal and external stakeholders

Assurance (see [Chapter 3.9 Assurance](#))

- I understand if the project is required to follow any of the NSW Government assurance processes

Evaluation (see [Chapter 8.1 Evaluation](#))

- I have started to plan how I will evaluate my project and considered what I need to do during the project implementation to ensure I can evaluate it effectively

Additional questions to consider include

- Launch strategy: I have decided whether the project will begin with a pilot or trial to test and prove a concept or start immediately with a full-scale launch
- Location logistics associated with equipment installation: I am aware of any issues that need to be addressed and customer needs to consider.

3.1.6 Additional resources

- The [Praxis website](#) has extensive resources on project management.
- AS/NZS ISO 9001:2016 *Quality Management Systems – Requirements* is an Australian standard identical to ISO 9001:2015. It specifies requirements for a quality management system (QMS). A QMS is a set of policies, processes, and procedures for planning and execution in the core business area of an organisation (i.e. areas that can impact the organisation’s ability to meet customer requirements).

4. Stakeholder engagement

4.1.1 What is effective stakeholder engagement?

Stakeholder engagement is vital for organisations to be able to understand and respond to the legitimate concerns of the various groups who may impact or be impacted by a project or decisions made.

Effective engagement is open, transparent and inclusive. It promotes healthy conversation and ensures that stakeholders feel they have been listened to. This can help build sustainable consensus and mandate for change.

Effective stakeholder engagement begins at the planning phase of your project and is revisited at major milestones in the life of the solution. Engagement is used to help validate your assumptions and ideas when decisions are being made. It can be informal or formal and ranges from sharing information to active consultation and co-designing solutions.

4.1.2 The importance of stakeholder engagement for IoT-enabled projects

The growing interest in IoT as an emerging technology and proliferation of IoT-enabled projects has resulted in a mix of myths, suspicion, and enthusiasm on the subject. This makes it extremely important to engage with stakeholders to ensure your IoT solution is understood and supported by those who affect or are affected by it, while still being designed and delivered to meet the project's intent.

The ubiquitous and often invisible nature of IoT means that stakeholders often do not realise they are stakeholders until they are negatively impacted, for example by a data breach. This makes proactive engagement particularly important to mitigate the impact of risks.

Proactive engagement can maximise the benefits of IoT. The data that IoT solutions generate may be useful beyond the direct project objective. Consultation on the development of data requirements can help you to clearly understand the purpose and benefit of your IoT data collection and use. This includes consultation with stakeholders who will consume the data you will produce or who will use the insights generated from your IoT solution, to ensure your approach meets their requirements.

Effective stakeholder engagement throughout your IoT-enabled project can allow you to:

- get diverse views on the issue you are trying to address and your proposed IoT solution
- design IoT solutions that genuinely meet your needs and your stakeholders' needs
- build clarity and consensus with those affected by your IoT-enabled project
- get buy-in from stakeholders to support the project
- identify potential issues that could disrupt the project

- manage stakeholder expectations
- maintain public trust through transparency and choice around data that is being collected and used
- identify opportunities for sharing and reuse of data and insights generated by your project.

Conversely, poor stakeholder engagement can jeopardise your project. It can increase the likelihood that your solution:

- does not meet its intended purpose
- is actively opposed
- does not integrate with existing systems
- breaches legislation or regulations
- increases business processes
- creates a negative user experience.

4.1.3 How to effectively engage stakeholders

There are five steps in the stakeholder engagement process:

- 1) Identify who your stakeholders are
- 2) Analyse your stakeholders to gain insights
- 3) Plan how you will engage with them to meet your objectives
- 4) Act on your plans, and handle any resistance you encounter
- 5) Review progress and re-engage to make further progress.

Five steps in the stakeholder engagement process



The five steps of stakeholder engagement are outlined below.

1) Identify your stakeholders

When preparing an engagement strategy, you will need to identify your stakeholders. Your stakeholders include any group or individual who might have an interest and/or is affected by your project. To help identify your stakeholders, ask yourself questions such as:

- Who will have an interest in the outcomes of the project?
- Who holds the knowledge that could be of value to the project?
- Whose views could influence the outcomes of the project?

Ensure you consider the life of your IoT solution, including project planning, installation, procurement and governance through to data collection, sharing and analysis, and technology maintenance. Typical stakeholders for an IoT-enabled project include:

- citizens
- government (from within or outside of your agency)
- external practitioners with experience delivering similar projects
- industry and business (including small businesses, corporates, non-government organisations)
- partners on your solution
- regulators, lobbyists, trade unions, and any other special interest groups
- your delivery team (including the IoT service provider(s)).

Typical stakeholders in an IoT-enabled project



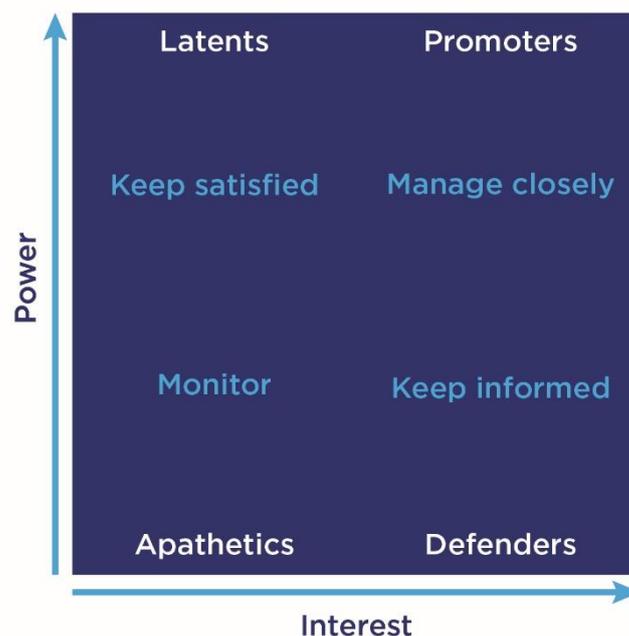
2) Analyse your stakeholders

Analysing your stakeholders will help you to understand their issues and concerns and allow you to tailor your engagement to make it as effective as possible.

The core elements of stakeholder analysis are outlined below, and can be recorded in a stakeholder register:

- sort your stakeholders by roughly quantifying their level of influence (power) and interest in your project and plotting it on a stakeholder matrix (see figure below)
- identify what you want or need from your stakeholders
- identify what you think your stakeholders want or need from you
- identify relevant elements of your stakeholders' background and interests
- assess stakeholders' attitudes and the potential impact on your project
- determine the strategy you will adopt to engaging with them.

Stakeholder matrix



3) Create an engagement plan

A stakeholder engagement plan provides clear direction for the engagement process and integrates with broader project planning and management. The plan should be monitored and revised as you develop your solution. The NSW Government has developed [A Guide to developing engagement plans](#) which can assist you.

To develop a stakeholder engagement plan, you need to:

- prioritise your stakeholders based on your stakeholder matrix

- tailor your engagement for each stakeholder, considering the message you want to convey and the contribution you want to elicit
- determine the method of engagement that will most effectively reach your stakeholder and elicit the desired response
- schedule your engagement with your stakeholders, including meetings and communications collateral.

Your method of engagement will be determined by the objective of the engagement and the stakeholder. Different stakeholders will be receptive to different engagement methods and styles based on factors such as demographics, location, size of the group and diversity.

Engagement methods

Situation	Engagement objective	Methods
Inform	To provide the stakeholder with balanced and objective information to assist them in understanding the problem, alternatives, opportunities and/or solutions.	<ul style="list-style-type: none"> • Correspondence • Newsletters/ bulletins • Fact sheets • Website • Social media • Blogs
Consult	To obtain stakeholder feedback on analysis, alternatives and/or decisions.	<ul style="list-style-type: none"> • Surveys • Interviews • Briefings • Focus groups • Online feedback tools • Diary studies • A/B tests • Tree testing
Involve	To work directly with the stakeholder throughout the project to ensure that their concerns and aspirations are consistently understood and considered.	<ul style="list-style-type: none"> • Workshops • Forums • Partnerships • Memoranda of Understanding (MOUs)
Collaborate	To partner with the stakeholder in each aspect of the project, including the development of alternatives and the identification of the preferred solution.	<ul style="list-style-type: none"> • Committees • Roundtables • Reference groups • Online collaboration tools
Empower	To allocate final decision-making responsibilities to the stakeholder	<ul style="list-style-type: none"> • Joint planning • Share responsibility • Sponsorships



For smaller scale and more experimental projects, consider an “incubator” approach (where a smaller group of stakeholders with direct impact and interest are consulted), rather than a broad approach like community consultation. An incubator approach can allow for “failing fast”, if necessary, without losing your momentum. Once a bigger scale rollout is deemed as feasible, a broad consultation process can proceed.

4) Act on your plan

Execute your plan. Record each action as you go to keep track of who you have engaged, when you engaged with them (i.e. the date) and under what circumstance (e.g. introduction email, workshop, interview).

This helps manage the process and is also a useful record that can be reflected on during the evaluation stage or to reassure project sponsors that an effective stakeholder management process was followed.

5) Review your progress

Stakeholder engagement should be an ongoing process. Stakeholders’ sentiments and levels of engagement will change as your project is developed, set up and goes live. Track these changes and reengage your stakeholders accordingly.

4.1.4 Additional resources

For further guidance on effective stakeholder engagement, see the below list of resources or contact your organisation’s communications team:

- Information and Privacy Commission NSW – [Charter for Public Participation – a guide to assist agencies and promote citizen engagement \(2018\)](#)
- NSW Government Department of Premier and Cabinet – [Preparing for effective engagement: A guide to developing engagement plans \(2012\)](#)
- NSW Government Better Regulation Division – [Stakeholder engagement strategy \(2016\)](#)
- Australian Government Department of Prime Minister and Cabinet – [Cabinet Implementation Unit Toolkit – Engaging stakeholders \(2013\)](#)
- UK Government Department for Business, Innovation and Skills – [Ensuring effective stakeholder engagement \(2016\)](#)
- [International Association for Public Participation.](#)

4.2 Data needs assessment

You need to undertake a data needs assessment in order to design the data requirements for your project. This is a multi-stage process and involves the considerations set out in this chapter.

4.2.1 Understanding your desired business outcome

You need to understand the business outcome you want to achieve through your IoT initiative so that you can design and build a data approach that safely and securely meets your business needs.

Start by determining what data you need to achieve your business outcome. Do this by defining specific questions you wish to answer then identifying the data needed to answer the questions.

To answer the question, ‘Which fields on a farm need irrigating?’, data can be collected on soil temperature and moisture content from sensors placed in the fields. Further insights can be generated by combining the data with meteorological data to avoid irrigating when rain is forecast. More valuable insights can be generated by analysing the data from the IoT solution with data from other sources, such as data from other farms or on commodity prices.

Data applications in a smart farming use case

IoT data level of sophistication	Example	Benefits
Raw data	A farmer puts sensors in fields to understand the temperature and moisture content of the soil.	Accurate real-time answers to: <ul style="list-style-type: none">• Which fields need irrigating?• Do we need to use fertiliser?
Combined data	The farmer combines MetService (NZ) weather data with soil temperature and moisture readings.	Ensures the irrigation systems will not waste precious water irrigating crops when rain is forecast.
Analytics	Sensors continuously monitor soil health and crop levels. New data sources are fed into the mix, such as aggregate data from other farms or commodity prices in the Asia Pacific. Predictive analytics provides insights from all this data using algorithms.	Accurate, real-time answers to: <ul style="list-style-type: none">• When should we sow seeds to get the greatest yield?• What fertiliser should we use?• When and what crops should we plant to get the biggest profit?

Source: Adapted from [Beca \(2018\)](#)



Tip: Consider the frequency of the data, including whether 'real-time' data is required. Collecting more data or more frequent data than is needed to achieve your business outcome can create a data processing and storage burden, and increased privacy and security risks.

Case Study – SA Water sensor deployment to improve services

SA Water, a water utility in South Australia, installed IoT sensors into its pipes as part of a [pilot program](#) to create a smart water network to monitor water flow and pressure and provide smart meters to customers. SA Water wanted to utilise the data collected from the IoT sensors to predict potential failures in its system and identify and address issues faster. It was the first water utility in the world to implement an IoT solution.

SA Water identified that these business outcomes required real-time data monitoring and analytics. Understanding their business needs led SA Water to develop a cloud-based data collection solution and a data analytics platform for notifications and visualisations. This enables the regulator to access real-time information about its systems drawn from the sensor-outfitted pressure sensors, water quality platforms and flowmeters.

Since installing IoT sensors in its pipe network, SA Water has used the data collected to prevent ten major water main failures, detect a 100 litre per minute leak and save one customer \$15,000 per month. The predictive maintenance and remote monitoring enabled by the project has allowed SA Water to make better data-driven decisions and created opportunities for cost-savings and future-proofing the network.

4.2.2 Engaging with stakeholders about data

Talking to business and community stakeholders will help ensure the IoT approach you design genuinely meets business needs. It can also assist with getting buy-in and fulfilling stakeholder needs:

- As you design your data requirements, consult with stakeholders including those who will use the insights generated from your IoT solution. This will help you understand the purpose and benefit of your IoT data collection and use, design an approach that is fit for purpose and delivers the best community benefit, and meets stakeholders' requirements while providing a good user experience.
- Seek public engagement on proposed IoT initiatives to maintain public trust by providing transparency and choice around what data is collected and how it will be used. Always consider whether your planned data uses are in line with your community's expectations and delivers value to the community.
- The data and insights generated from your project may be useful for purposes other than those originally intended. Consult as broadly as possible to identify these opportunities so that data sharing and reuse opportunities can be incorporated into your project design.

4.2.3 Limitations in your operating environment

IoT works best when combined with existing business data and data environments; it has the potential to unlock significant value and customer outcomes. Do your best to make sure that data about key processes can be easily integrated from across different business areas and data sources across your organisation, to generate maximum insights.

Make sure you understand and address any issues with your operating environment that may inhibit your ability to use the data generated by your IoT initiatives and to integrate this data with your work processes. Key data-related inhibitors to IoT success are:

- inflexible legacy architectures
- lack of consistent standards
- low cyber security maturity levels
- interoperability challenges
- inconsistent data formats, terminology, capture standards, and quality requirements
- inflexible provision of data from IoT service providers.

4.2.4 Improving data governance and management practices

Good data governance, management, and practice need to be designed and built-in from the beginning so that the data generated is useful, accessible, secure and of dependable quality.

Data management and governance processes must be rigorous for new IoT generated data as well as existing business data so that the data can be combined. The better the quality of existing business data, the easier it is to integrate with IoT data to generate richer and more relevant insights.

You cannot use data with inconsistent formats or definitions and expect IoT processes and applications to make sense of it or use it to train artificial intelligence. You need to create a solid and useful data platform first. Similarly, vendor lock-in, where an IoT service provider restricts access to data or the way it can be used, can be just as costly in the long run as a major data breach or system failure.

Much of the data sitting in existing systems are siloed, not only on-premises but also in various cloud silos, third-party datacentres, on personal devices, in legacy environments, and all contained in various formats and data standards. Identifying high-value data in these environments, centralising and standardising it and making it available to your IoT initiatives can add significant value to these initiatives.

Revised organisational policies on data governance and management may need to be established to ensure that high quality and relevant business data is captured, stored, secured and used, and is available in formats and standards that enable its interoperability and use across the organisation. To support this and facilitate consistent practices across government, government policies, standards and processes are available via the [Data.NSW Program](#).



Tip: Prioritise data consistency and standardisation across your organisation in the manner that best caters to your organisation's needs - there is no one right way. For example, one approach is to create a centralised data office in your organisation, and a single authority or point of truth for data advice and standards.

4.2.5 Data requirements specification

You need to design your data requirements specification as part of your data needs assessment. Follow the steps below to specify your basic data requirements, in addition to any other data requirements relevant to your project.

1) Describe the data to be collected

Describe the data to be collected from IoT sensors or devices (e.g. measurements such as temperature, soil moisture content, water pressure or blood glucose levels) and from other data sources.

2) Specify the metadata of your data

Metadata is 'data about data'. Specify metadata to ensure the data you collect is meaningful, [interoperable](#), and can be compared with other data sources within your organisation and externally.

Depending on the data, metadata may include:

- the unit of measurement (e.g. degrees Celsius for temperature)
- the frequency of measurement (e.g. every 10 minutes, every hour, once a day)
- the format
- any rules to be applied to the data.

3) Specify the device metadata

In addition to specifying data metadata, it is important to specify [metadata for the IoT devices](#) that collect the data. Device metadata can be used to negotiate communications protocols between devices and enable interoperability. It can also be used to map legacy devices and achieve ongoing compatibility and accessibility of older data sources. Device metadata may include:

- sensor make and model
- class or type
- manufacturer
- date manufactured
- serial number
- revision
- physical location of the device (See [Chapter 6.2 Spatial data requirements](#))
- calibration of the device

- power source (e.g. battery)
- wireless network (e.g. 5G enabled)
- protocols for storing and sharing the data.

4) Determine your data model

The data model/structure should be clearly defined and documented. Seek common data models for the exposure of data, either privately or where appropriate publicly. They can adhere to international standards or emerging frameworks developed by other international bodies (e.g. FIWare and Open & Agile Smart Cities for Smart City-related IoT data). Other sector-specific standards and guidelines relating to safety, security, and privacy should also be used.

The information security classification of the data should also be determined and recorded in accordance with the [NSW Government Information Classification, Labelling and Handling Guidelines](#).

5) Define data quality

The data specification should also define data quality requirements to ensure the data generated in your IoT-enabled project is fit for purpose.

Organisations need to establish well-governed processes to ensure their IoT data is of sufficient quality for use and re-use. Data quality assessment processes should be automated (where possible).

4.2.6 Design and configuration for data collection

You may need to work with service providers to design devices and software configuration so that the required data can be collected and used.

IoT sensors are precisely calibrated devices designed to gather specific data over time. The number and frequency of observations multiplied by the number of sensors will dictate the rate at which data is accumulated and the storage needs.

4.2.7 Data analytics

The analytics you use will depend on the outcomes you wish to achieve. These may be:

- descriptive ('What happened?')
- diagnostic ('Why did it happen?')
- predictive ('What will happen?')
- prescriptive ('What action could be taken?')
- cognitive ('What is the best action?').

Consider if the analytics and presentation of insights provided with the device or sensor meet your needs or if you will need to develop a bespoke solution.

If you intend to use data from another source, consider how you will integrate that data with your IoT data.

4.2.8 Data retention

IoT generates vast amounts of data depending on the size of sensor networks and the complexity and frequency of observations. To avoid large storage costs (or to minimise the risk of premature data destruction) conduct a business, risk, accountability and customer needs assessment to identify considerations that apply to the retention and destruction of data. This includes considerations such as:

- Is there personal data in your IoT transmissions? If so, under the [Privacy and Personal Information Protection Act 1998 \(NSW\)](#), personal information should be destroyed as soon as the objective it was collected for is completed (but note that if it is a state record then the rules in the *State Records Act 1998* (NSW) will also need to be considered).
- 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 data that is not needed for ongoing purposes.
- Are there any audit or accountability requirements applying to your IoT process?

The [State Records Act 1998 \(NSW\)](#) sets the rules for how long government information needs to be retained. Depending on the business purpose of your project, your IoT data will have different legal retention and destruction requirements. Refer to the [NSW State Archives and Records website](#) for more information.

You need to consider how to create a cohesive and connected record if the IoT data needs to be retained for a longer-term. This can be difficult to achieve between generations of sensors. To create a persistent, longitudinal record, you may need to reduce the frequency or precision of observations in order to match time-series at an equivalent level of detail. Document any decisions of this type in a data quality statement.

All retention and destruction decisions need to be authorised and documented to achieve transparency and accountability over the destruction of government information assets.



Tip: If you are working with multiple service providers, make sure they can all support and deploy the data retention and destruction frameworks you require for your project.

4.2.9 Data storage

You need to decide on suitable storage for data generated by your IoT initiative. Storage requirements for data produced via IoT networks will grow over time so storage models need to be considered as a key dependency in long-term solutions.

The storage you choose will depend on your data requirements. Considerations include:

- how quickly the insights are needed (e.g. real-time)

- type of data and the bandwidth required (e.g. video)
- level of connectivity (e.g. offline processing)
- level of security.

Storage will also be impacted by IoT data flows. Various data flow scenarios are possible:

- sensors send their data to a central cloud server for analysis and storage
- sensor data may be pre-processed (cleaned, filtered and/or aggregated) by local devices before sending it to a remote server
- data flows from peer to peer for example, a sensor supplying data to an actuator.

The fidelity of wireless communications between devices is also important in understanding what the requirements for the architecture are, and where processing should be done. Reliability of transmissions is an important consideration.

In terms of data retention and associated storage costs, one approach is to engineer so that sensor data is only transmitted when there is change from the previous transmitted value. This requires some simple edge processing capability and is increasingly becoming more common practice.

Storage options include cloud, government data centres, and fog or edge computing. The latter is becoming increasingly important for IoT data as they tackle some of the issues associated with latency, bandwidth, security, and offline access. They are considered below.



Tip: IoT environments may not only produce data but also consume data from other sources. If this applies to your circumstances, factor this into your data storage arrangements.

a) **Cloud storage**

Cloud servers are a necessary environment for managing and storing the huge volumes of data generated by IoT devices. Leveraging the cloud is essential for data storage, easy sharing, and accessibility. Choosing cloud-based platforms can help to scale IoT initiatives but there may be additional costs associated with accessing and processing stored data.

The [NSW Government Cloud Policy](#) allows NSW Government agencies to store data in the cloud as long as the agency has considered the risks of the approach and selects a supplier of cloud storage services that can address those risks. If you want to use a cloud service provider recognised by [buy.nsw](#) to centralise your IoT data management, ensure there is direct bi-directional device connectivity, collaboration between hardware and cloud providers to achieve seamless end-to-end integration, or at a minimum, build a forwarding layer from the device-hosted cloud to the cloud service provider (if required).

Storing data and information in the cloud is allowed under the [State Records Act 1998 \(NSW\)](#) provided all legal information management responsibilities under the Act are met.



Tip: [buy.nsw](#) is a subset of the services available under the [NSW Government ICT Services Scheme](#) for procurement. Suppliers on the ICT Services scheme may elect to be included in the [buy.nsw](#) listing for cloud suppliers. Use of [buy.nsw](#) is not mandatory.

b) Data centres

Long term storage of data in data centres incurs long term costs and may have environmental impacts. Reducing the amount of data you keep can help minimise any environmental impacts. You can do this by implementing the legal data destruction authorisations under the [State Records Act 1998 \(NSW\)](#) and only keeping IoT data for as long as required to support business, customer and legal requirements.

c) Fog computing and edge computing

It can be inefficient to stream the increasing volume and velocity of data generated by IoT sensors and devices to the cloud and data centres. Fog and edge computing involve processing and analysing the data physically close to or within the sensor or device. This is beneficial if a loss of connectivity to the cloud is an issue (e.g. in regional or remote areas), insights are needed in real-time (e.g. in a healthcare setting) or bandwidth is not adequate to transmit the data to the cloud (e.g. if a video is being processed).

For example, connected diabetes devices often use fog computing or edge computing because diabetes patients require a rapid response to sensor input and cannot tolerate delays for cloud computing.

Fog and edge computing involve different architecture for typical data centres. Please speak to resources who have the relevant expertise before attempting to deploy this type of architecture.

[Advantages of fog and edge computing compared to cloud computing](#) include:

- greater data transmission speed
- less dependence on limited bandwidths
- greater privacy and security
- greater control over data generated in foreign countries where laws may limit the use or permit unwanted governmental access
- lower costs because more sensor-derived data is used locally, and less data is transmitted remotely.



Tip: Good cyber security cannot be resolved by device proximity to the source alone. Ultimately good cyber security comes down to organisational cyber maturity and good management. See [Chapter 3.6 Cyber Security](#) for advice.

4.3 Risks and obligations

This chapter provides a framework for the management of risks and obligations related to IoT-enabled projects. The advice provided here is general in nature. See other chapters in this policy guidance for information on specialised risk types, such as privacy, data, cyber security, and procurement risks.

4.3.1 What is risk and compliance management?

a) Risk, compliance and obligations

Risk is ‘the things that could potentially happen’, either in a positive or negative sense, that would impact your ability to implement and deliver a project. Risk management is how you manage the uncertainty of potential risks. It involves the identification, analysis, and evaluation of a project's risks and the development of cost-effective strategies to treat those risks.

Compliance refers to ‘the things that we must do’ when managing a project, which can come from legislation, policies, codes, contracts, standards and other practices which are imposed or adopted – these are known as obligations.

Projects of all types and sizes are subject to internal and external influences and obligations that can present risks. In some instances, risks can provide opportunities for the project, such as delivering the project earlier than expected, cost savings or innovative designs. However, if risks are not adequately managed, they may cause disruption or failure of the project.

b) What does this mean for projects involving IoT?

Projects which involve IoT are susceptible to a wide range of risks due to the connected nature of IoT and the rapid pace of technological change. Without proper caution, a network is only as strong as its weakest link. Also, the bigger the network, the more exposed the project is to risks.

Teams deploying IoT-enabled projects need to understand their obligations and risk appetite and to make decisions accordingly from the beginning of a project. Risk appetite is the amount and type of risk you are willing to take in order to achieve your project objectives. Risk appetite is often specified at the enterprise level for your organisation.

Examples of risks a project using IoT may face

Risk type	Description	Relevance to IoT	Relevant policy/ legislation	Practical tools	Further information
General	Things that can potentially happen, either in a positive or negative sense, which can impact your organisation, work or project	Like any project, IoT-enabled projects are subject to risks	<ul style="list-style-type: none"> • Internal Audit and Risk Management Policy for the NSW Public Sector (2015) • NSW Auditor General's report - Internal Controls and Governance (2018) • Audit Office of NSW Risk Management Framework (2018) 	<ul style="list-style-type: none"> • NSW Treasury Risk Management Toolkit (2012) • Pre-mortem exercise 	Chapter 3.4 Risks and obligations
Cyber	Harm/loss resulting from a breach or attack on information systems	IoT devices are connected by their nature and therefore vulnerable to cyber security risks	<ul style="list-style-type: none"> • NSW Cyber Security Policy (2019) • ISA/IEC 62443 Cybersecurity Certificate Programs 	<ul style="list-style-type: none"> • NSW Treasury Risk Management Toolkit (2012) • Pre-mortem exercise 	Chapter 3.6 Cyber Security
Privacy	Harm/loss resulting from failure to comply with privacy obligations	IoT devices that collect information must comply with NSW Government privacy obligations	<ul style="list-style-type: none"> • Privacy and Personal Information Protection Act 1998 (NSW) • Privacy Act 1988 (Cth) • Health Records and Information Privacy Act 2002 (NSW) 	<ul style="list-style-type: none"> • NSW Treasury Risk Management Toolkit (2012) • Pre-mortem exercise • Privacy Impact Assessment 	Chapter 3.5 Privacy
Contract	Failure to manage IoT service providers and supply chain obligations leading to unfulfilled contracts and/or other adverse outcomes	IoT-enabled projects that involve procurement require the use of contracts	<ul style="list-style-type: none"> • NSW Government Procurement Guidelines - Risk Management (2006) 	<ul style="list-style-type: none"> • NSW Treasury Risk Management Toolkit (2012) • Pre-mortem exercise 	Chapter 5.1 Procuring IoT solutions

Risk type	Description	Relevance to IoT	Relevant policy/ legislation	Practical tools	Further information
Data	Harm/loss due to poor data governance, data mismanagement and/or lacklustre data security	Many, if not most, IoT-enabled projects which rely on IoT involve the collection and use of data	<ul style="list-style-type: none"> • NSW Government Cloud Policy (2018) • NSW Cyber Security Policy (2019) • NSW Data and Information Custodianship Policy (2013) • Data Sharing (Government Sector) Act 2015 (NSW) 	<ul style="list-style-type: none"> • NSW Treasury Risk Management Toolkit • Pre-mortem exercise • Privacy Impact Statement 	Chapter 3.6 Cyber Security Chapter 3.5 Privacy
Procurement	Failure to perform due diligence leading to ineffective spend and poor outcomes	Almost all IoT-enabled projects will involve a procurement process	<ul style="list-style-type: none"> • NSW Government Procurement Guidelines - Risk Management (2006) 	<ul style="list-style-type: none"> • NSW Treasury Risk Management Toolkit • Pre-mortem exercise 	Chapter 5.1 Procuring IoT solutions
People safety (WHS)	Harm (death, injury or illness) resulting from exposure to a hazard	Most relevant to IoT enabled projects involving physical infrastructure	<ul style="list-style-type: none"> • SafeWork NSW codes of practice 	<ul style="list-style-type: none"> • SafeWork NSW codes of practice 	SafeWork NSW
Legislation/ obligations	Lack of awareness and resources for the management of obligations resulting in requirements not being met	All projects, including IoT-enabled projects, are subject to legislation, obligations, and risks	<ul style="list-style-type: none"> • For example, Government Sector Finance Act 2019 (NSW); Environmental Planning and Assessment Act 1979 (NSW) 	<ul style="list-style-type: none"> • NSW Treasury Risk Management Toolkit • Pre-mortem exercise 	Chapter 3.4 Risks and obligations
Technology	Harm/loss resulting from rapid technology changes/failures or lack of interoperability	IoT-enabled projects involve technology	N/A	<ul style="list-style-type: none"> • NSW Treasury Risk Management Toolkit • Pre-mortem exercise 	Seek advice from experts within your organisation
Machinery of Government	Project barriers resulting in changing priorities and workstreams	Change of leadership and priorities can impact IoT-enabled projects	N/A	<ul style="list-style-type: none"> • NSW Treasury Risk Management Toolkit • Pre-mortem exercise 	Chapter 3.4 Risks and obligations

4.3.2 How to manage risk and compliance

Effective risk and compliance management allows you to identify your project's strengths, weaknesses, opportunities, and threats and helps you to make effective decisions. This increases the likelihood of your project achieving its objectives.

Risk and compliance management is proactive. It should be embedded as part of the management of a project. A risk and compliance assessment can help the project team to identify the internal and external obligations and risks a project faces, and outline actions to manage or treat them.

Follow the steps below to manage risk and compliance in your IoT-enabled project. Steps 2 to 4 are the risk assessment process. Also, be sure to speak to your organisation's risk and compliance team and/or Project Management Office about any internal risk and compliance management policies and requirements. They can help you implement the recommendations in this chapter.

1) Understand

The first step is to understand your obligations and the implications for your project activities, products, and services. Think about the internal and external context of your project, such as:

- What is the scope of your project?
- What are the dependencies?
- Who are the stakeholders and what are their goals?
- Do you have any assumptions going into this project?
- What amount and type of risk can your project take? This should align with your agency's risk appetite.
- Have you met your compliance requirements and/or other obligations that may be applicable to your organisation?

2) Identify

This step is about identifying and describing risks that might prevent your project from achieving its objectives. Alternatively, your project may provide intended or unintended opportunities for your team, organisation or others.

Do not be afraid to look outward. Consider risks that may come from outside your organisation, such as climate or weather-related risks, or economic risks. Be aware that risks may impact people or projects not directly involved in your project, particularly in the case of cyber security and privacy risks. A pre-mortem exercise can assist with identifying and mitigating risks through an interactive activity with your team. See [Appendix A](#) for steps to run a pre-mortem exercise.

Identified opportunities and risks should be recorded and reported in a project Risk Register. You can find a Risk Register template in the [NSW Treasury Risk Management Toolkit](#).

3) Analyse

Risk analysis involves detailed consideration of uncertainties, risk sources, consequences, likelihood, and controls. Analyse the risks to determine their causes, probability of occurring and the likely consequences.

4) Evaluate

Evaluation involves reviewing the risks that have been identified and analysed against any established risk criteria for your organisation. Some risks will have a small impact on the project and the organisation. Some may result in a project prematurely ending. Others may impact people and projects outside of your project and organisation.

Evaluating and prioritising risks against your risk appetite helps to determine what resources you should allocate to mitigating each risk, and what level of risk is acceptable. You should update your Risk Register to reflect the outcomes of the risk evaluation.

5) Treatment

You need to consider what actions could be taken to address each of the identified risks. A risk may be accepted, mitigated or eliminated. Balance the potential benefits against the cost, effort or disadvantages of implementing the treatment. Assign owners to each action who is accountable for mitigating the risk.

Record each action and the owner in the Risk Register. Clearly identify the order in which the actions should be taken, as well as the rationale for the action, resources required, reporting, measures, and constraints.

4.3.3 Ongoing communication and monitoring

Ongoing communication and consultation are vital to ensuring your stakeholders understand the risks of your project, the basis on which decisions are made, and why particular actions are required.

Also, remember to monitor the Risk Register throughout the project to ensure you are completing the risk mitigation actions. Existing risks may be eliminated by taking effective action.

You should consider risk and compliance reviews at different points in the project since risks change throughout the lifecycle of a project. This can be just a simple review of existing information in the Risk Register. Any new risks which are identified should be added to the Risk Register.

4.3.4 Risk management standards

Organisations should comply with international standards that Australia has adopted. Key standards relevant to risk management are summarised in the following table.

Risk management standards	Description
AS/NZS ISO 31000:2018 Risk Management - Guidelines	This Australian standard is the most widely used standard for risk management in the NSW Government. It is equivalent to ISO 31000:2018. It provides customisable guidelines on managing risks and guidelines on compliance management.
AS ISO 19600:2015 Compliance Management System – Guidelines	This Australian standard adopts ISO 19600:2014 to provide guidance for establishing, developing, implementing, evaluating, maintaining and improving a compliance management system.
AS ISO 22301:2017 Societal Security – Business continuity management systems – Requirements	This Australian standard is equivalent to ISO 22301:2012. It specifies requirements for a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
AS ISO/IEC 38500:2016 IT – Governance of IT for the Organisation	This Australian standard is equivalent to ISO/IEC 38500:2015. It provides guiding principles on the use of IT within organisations. It comprises a framework of definitions, principles and a model.
AS ISO/IEC 38505.1:2018 IT – Governance of IT – Governance of data – Application of AS ISO/IEC 38500 to the governance of data	This Australian standard is equivalent to ISO/IEC 38505-1:2017. It provides guiding principles on the application of the AS ISO/IEC 38500 model to the governance of data.
ISO/IEC 27031:2011 IT – Security techniques	Not adopted by Australia, but this international standard provides a framework for improving an organisation's ICT readiness to ensure business continuity.

4.4 Privacy

4.4.1 The privacy regulatory landscape

Privacy regulation in Australia focuses on the handling of 'personal information'. This is information about an individual or information that can reasonably be linked to an identified individual or used to identify an individual. The handling of personal information is regulated at both the state and federal level. In NSW the [Privacy and Personal Information Protection Act 1998 \(NSW\)](#) (PIIP Act) and [Health Records and Information Privacy Act 2002 \(NSW\)](#) (HRIP Act) apply to NSW Government agencies, NSW local government, and public universities. The PIIP Act defines [personal information](#) and sets out 12 [Information Protection Principles](#) (IPPs) that govern the handling of personal information. The HRIP Act sets out 15 [Health Privacy Principles](#) (HPPs) governing health information.

The [Privacy Act 1988 \(Cth\)](#) (Privacy Act) applies to most Australian Government agencies and some private sector organisations, including private universities and health service providers. There is an exemption for small businesses with an annual turnover of less than \$3 million. The Privacy Act defines personal information for Commonwealth purposes and sets out 13 [Australian Privacy Principles](#) (APPs).

The privacy laws give individuals rights over the way their personal information is handled. They allow the individual to:

- know why personal information is being collected and how it will be used or disclosed
- access and correct personal information about themselves
- make a complaint.



Tip: Collecting periodic or ongoing information can build a pattern of usage which, if linked to a person, can be personal information.

a) Surveillance and telecommunications

Data surveillance devices, listening devices and tracking devices in NSW are regulated by [Surveillance Devices Act 2007 \(NSW\)](#) and, in relation to workplaces and employee use of workplace resources, the [Workplace Surveillance Act 2005 \(NSW\)](#).

Some IoT devices or uses of IoT services may be in the scope of these surveillance laws (in addition to the abovementioned privacy laws). The surveillance laws require notice to be given to affected individuals, and in some cases their affirmative express consent.

Also, be aware of the [Telecommunications \(Interception and Access\) Act 1979 \(Cth\)](#) that protects the privacy of individuals using the Australian telecommunications system. It prohibits the interception of, or access to, communications except in specified circumstances.

b) European General Data Protection Regulation Requirements

The European Union's General Data Protection Regulation (GDPR) requirements may impact your IoT service provider. It may impose contractual conditions relating to compliance with GDPR requirements if your IoT service provider is impacted. The [Office of the Australian Information Commissioner](#) (OAIC) and the [Information and Privacy Commission NSW](#) (IPC) have information on how to understand the impact of the GDPR on your organisation.

4.4.2 Privacy and IoT

a) Personal information collected by IoT

Data collected using IoT sensors may contain personal information if it:

- is about an identified person.
- can 'reasonably' be linked to an identified person. Information is 'reasonably identifiable' if there is a reasonable likelihood that re-identification can occur.
- can be used to identify an individual
- is held by an organisation with the capability to identify the information, even if the organisation has not yet done so.

For example, when counting how many cars drive through an intersection:

- if a road sensor registers when a vehicle drives over the sensor but does not collect any other information, that information in isolation is unlikely to be personal as it cannot be linked to the car or driver
- if CCTV footage of the road is available and it is possible to match the timestamps from the footage to the sensor data, it may be possible to associate sensor data with images of the car and driver. If so, that data is personal information.

Whether a person is reasonably identifiable is assessed in the circumstances of the case. Relevant considerations include:

- the nature and amount of information collected and held
- who will hold and have access to the information, including their skills and abilities and the resources available to them?
- any other information that is available that could be matched or referenced against your information, and the practicability of using that other information to identify an individual.

See also the [IPC's fact sheet on reasonably ascertainable identity](#).

b) Managing IoT data

Data management is more difficult with IoT data due to the volume of data and dispersed data sources and entities processing data. It is important that data volume, frequency, and capture methods do not create unintended consequences.

To illustrate this concept, consider sensors placed on the exterior wall of houses in a specific area to monitor air quality and temperature. If the devices are configured to capture a continuous or high-frequency data feed, fluctuations in air temperature may make it easy to identify when people are in or out of the house. The privacy impacts can be minimised by decreasing the frequency of data capture, aggregating the data to a street or suburb level when it is captured, or relocating sensors to less sensitive locations nearby.

c) Commonwealth privacy legislation and IoT-enabled projects

An IoT-enabled project may be subject to both NSW and Commonwealth privacy legislation. For example, if a NSW government agency procures sensors and a system that record identifiable traffic data, the IoT service provider needs to comply with the *Privacy Act* while the NSW Government agency needs to comply with the PPIP Act. The NSW Government agency is also required to ensure the IoT service provider does not breach NSW privacy laws.

You need to consider how to protect personal information if you are working with an entity that is not covered by any privacy legislation. This can be done through contract provisions that address the handling of personal information and appropriate data governance.

4.4.3 Privacy obligations around collecting and holding data

a) Obligations around personal information

Once information is collected (personal or de-identified) you have obligations on the way you hold and allow access to it. It is recommended that you do not collect personal information (unless necessary) as it is subject to stricter storage and access requirements under the IPPs.

b) ISO/IEC 29100:2011 IT – Security techniques – Privacy framework

ISO/IEC 29100:2011 relates to privacy. This international standard has not been adopted in Australia, but its provisions are a useful guide on how to keep personal information secure.

c) Identified versus de-identified data

De-identifying identified data can reduce privacy risks, though it is not a panacea for sound privacy practices. Effectively de-identified data is not personal information within the meaning of the PPIP Act, HRIP Act or Privacy Act.

You must consider the risk of reidentification before you release or share de-identified data – can the data be linked to identified individuals using other information or data that is available?

Remember that if you reuse or recycle data sets over multiple projects there is a risk of being able to identify someone by linking the datasets together. The OAIC and Data 61 have published a practical [De-identification Decision Making Framework](#).

Case Study – Department of Health data re-identification

In 2016 the Commonwealth Department of Health published data online related to the Medicare Benefits Schedule and Pharmaceutical Benefits Scheme. The de-identified information was released for public interest and medical research and policy development purposes.

Within a month of the dataset release, the Department of Health was advised that by linking datasets this de-identified information set could be used to identify people. The dataset was removed from public access.

The Australian Privacy Commissioner considered that the Department had breached the APPs by publishing the dataset. The situation could have been avoided by:

- not releasing the data as it was once identifiable
- better de-identification processes
- better data encryption
- making the data less area specific.

This case demonstrates that data from one data set can be matched with another which can reasonably identify an individual. See the [OAIC](#) website for more information.

d) Privacy Management Plan

Familiarise yourself organisation's Privacy Management Plan (a strategic planning document describing how the organisation will comply with the PPIP Act and HRIP Act). Every NSW Government agency and local council is required to have one.

e) Privacy Collection Statement

Section 10 of the PPIP Act requires you to inform individuals if you are collecting personal information, why you are collecting personal information, what the information will be used for and how they can view or amend their personal information. You must make individuals aware before, or as soon as is practical after, the personal information is collected.

The PPIP Act does not require this notice to be given in a specific way so you need to consider the best way to communicate with your audience. For example, you can post a prominent sign, send an email to the affected individuals, or publish a Privacy Collection Statement on your website. A template Privacy Collection Statement is at [Appendix B](#).

4.4.4 Best practice – Privacy by design

a) Principles of privacy by design

Privacy by design is the process of proactively identifying privacy risks during the development of a project or initiative so that risks can be mitigated as part of the design of

the project. Privacy by design allows privacy to be 'baked-in' from the beginning so that your IoT solution is privacy-protective by default.

Consider these [seven principles of privacy by design](#) when rolling out an IoT solution:

- 1) Be proactive, not reactive. Be preventative not remedial. Do not wait until there is a privacy breach to consider privacy.
- 2) Privacy as the default setting. Think privacy first and foremost.
- 3) Embed privacy into the design of your project
- 4) Positive sum, not zero-sum – think win/win. Can you find a solution which has the greatest benefit e.g. data generation and analytics with strengthened privacy feature?
- 5) End to end security for full lifecycle protection.
- 6) Visibility and Transparency. Be open with stakeholders.
- 7) Respect for user privacy. Keep it user-centric.

Case Study – Privacy by design by Byron Bay Shire Council

In [DAB v Byron Shire Council \[2017\] NSWCATAD 104](#) a resident of Byron Bay Shire Council complained to the NSW Civil and Administrative Tribunal that the Council's new 'pay by plate' parking scheme breached the IPPs under the PPIP Act. Under the scheme, people were required to enter their name, address, licence plate and other details into a web portal. The data in the portal was transmitted to two servers. One server contained all the information, the other service only contained the exempt licence plates.

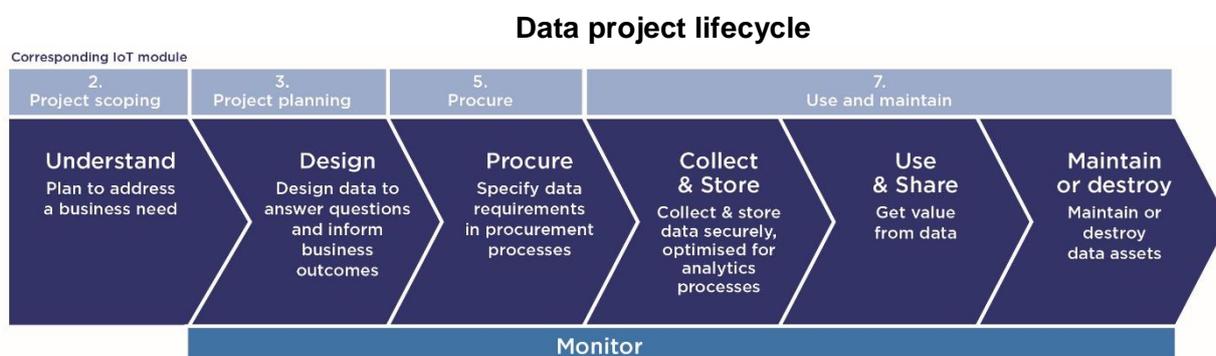
The resident argued that by requiring individuals to enter their licence details, their personal information was being collected and could identify them.

The Tribunal found that it was very unlikely that the identity of an exemption holder could practically and reasonably be ascertained from the information, whether by comparison with other data held by the Council or otherwise. The Tribunal also found that a licence plate number entered into a parking meter without any other data, was not information about an individual. This meant the Council's handling of the information was not a handling of personal information regulated by IPPs.

Byron Bay Shire Council had applied privacy by design by creating two data silos, ensuring that the database which contained residents' personal information was siloed from the licence plate information for the parking meters.

b) Implementing privacy by design

Mapping the way that data flows through your project – who holds it and how they handle it – can help you identify the privacy risks inherent in your project and implement privacy by design. It is important to monitor the creation, use, and access to data to ensure appropriate and secure usage, and to identify unexpected or nefarious patterns of use.



The table below sets out considerations for each stage of the data project lifecycle to help you implement privacy by design.

Data project lifecycle stage	Things to consider
Understand	<ul style="list-style-type: none"> Know the business outcome you want to achieve. This will determine the data you need.
Design	<ul style="list-style-type: none"> Consider IoT within the context of the NSW and Commonwealth Privacy, surveillance and information access laws. Check your organisation's privacy management plan. Conduct a Privacy Impact Assessment if personal information is involved. Minimise acquisition of personal information. If you need to collect personal information, identify the minimum number of data types, minimum data collection frequency and the minimum duration of data collection needed to achieve business objectives. Determine how you will notify participants you are collecting their personal information. If you need their consent, determine how consent will be obtained. Successful IoT initiatives usually involve a combination of hardware, software, and connectivity, which is then tied into business processes and operations. Data needs to flow, be added to, interpreted and then potentially flow back through this loop to trigger action. Understand this data flow and be clear about your data ownership and use rights in all elements of this flow.

Data project lifecycle stage	Things to consider
	See also Chapter 3.3 Data needs assessment .
Procure	See Chapter 5.2 Data considerations for contracting .
Collect & Store	<ul style="list-style-type: none"> • Minimise the data you collect. Only collect what you need, and do not collect personal information if you do not require it. Avoid collecting fine-grain data that identifies specific detail like a residential address. Instead collect low grain data, like a street, suburb or postcode. • De-identify data where possible. • Inform stakeholders and the public if you are collecting their data, why you are collecting it, and provide assurance that it will be used only for that purpose. • Separate your data sources so they are not all connected. Connecting data sources may identify additional data or create new information. • If there is a requirement for physical storage, consider the kind of physical storage medium you will use and how you will protect it from loss or misuse. • Control who has access to the data, provide personal logins and log who has access to the data. Consider having various levels of access, review all outputs for potential derived or inferred reidentification. Appoint a data custodian specific responsibility for applying these strategies. This could be at an organisational, program or project level. • Enforce the rules of access and apply your Privacy Impact Assessment and management framework. Implement audit mechanisms to verify that only authorised users are accessing data and for authorised purposes.
Use & Share	<ul style="list-style-type: none"> • Display an up to date Privacy Collection Statement on your website and/or within the physical area that you are using sensors to collect data. • Use personal information for the primary purpose for which it was collected. • Consider if the uses of the data are changing or evolving and whether secondary use is permitted. • Determine if you require additional consent to share information or if sharing is permitted. Share de-identified data rather than personal information where possible. Consider what process will be applied to de-identify the information, and the risk of re-identification.

Data project lifecycle stage	Things to consider
	<ul style="list-style-type: none"> • Present and share aggregated rather than specific results and identify whether applications can share aggregated rather than raw data. Consider whether aggregating a variety of data sources has the potential to re-identify individuals.
Maintain or destroy	<ul style="list-style-type: none"> • Securely destroy or de-identify data that you no longer require for a lawful purpose. • Minimise retention of personal information. Data should only be kept for the period needed to perform the nominated tasks. <p>See also the Data retention and destruction section.</p>

c) Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a written assessment of an activity or function that:

- identifies the impact that the activity or function might have on the privacy of individuals
- sets out recommendations for managing, minimising or eliminating that impact.

A PIA ‘tells the full story’ of a project from a privacy perspective. It is essential to operate on a privacy by design basis. A PIA should be conducted early in project development to guide implementation.

PIAs can help assess the overall *proportionality* of a policy or project, that is, whether the use of personal information strikes an appropriate balance between the project objectives and the resulting privacy impacts. This is particularly important where individuals do not have a meaningful choice to provide the information (i.e. where the collection of information is by sensors of which they are unaware, is required by law, or is required to access essential government payments or services).

The IPC has published a [Guide to Privacy Impact Assessments in NSW](#).

d) Privacy Self-Assessment

The IPC has published [Information Governance Agency Self-assessment Tools](#). These tools may be useful to self-assess privacy management in your organisation. The IPC recommends regular self-assessment.

4.4.5 Privacy access requests and GIPA requests for information

Requests for information can fall under either the PPIP Act or the [Government Information \(Public Access\) Act 2009 \(NSW\)](#) (GIPA Act) depending on the applicant and type of information or data being requested.

Under the PPIP Act, if you collect personal information you need to make it accessible to the individual and allow them to correct or amend their personal information as required.

Also, consider the impact of having a sensor network and the additional requests for aggregated data under the GIPA Act. Your organisation's Privacy Management Plan (and possibly your PIA) needs to have mitigation strategies in place if someone's personal information is unintentionally released under a GIPA request.

4.4.6 Managing a data or privacy breach

A data or privacy breach occurs when there is a failure that has caused (or has the potential to cause) unauthorised access to your organisation's data. Breaches include hacking and malware, sending an email containing classified information to the wrong person, and loss of a paper record, laptop or USB stick.

NSW does not currently have a mandatory notifiable data breach reporting requirement, however one is currently being developed (due in 2021). The NSW Privacy Commissioner has a [voluntary scheme](#) in place.

Check if your organisation has a data breach management or response plan in place. The OAIC has published [guidance on data breach preparation and response](#).

4.4.7 Links for further information

Visit the [Information and Privacy Commission NSW website](#) for guidance on implementing your privacy obligations under the PPIP Act and the IPPs and/or the HPIP Act and HPPs.

Visit the [Office of the Australian Information Commissioner website](#) for guidance on the Privacy Act.

4.5 Cyber Security

4.5.1 Securing IoT

This chapter outlines the guiding principles and best practices for implementing IoT to ensure protection against threats to confidentiality, integrity, availability and safety. It does not replace obligations to adhere to your organisation's information security policies if any.

Case Study – The growth of cyber security risks from IoT

The growth of IoT networks presents a range of risks and challenges. Some of these risks have been realised, and new risks and vulnerabilities identified. Examples include:

- [Princeton University researchers](#) developed a proof-of-concept named BlackIoT which allows an adversary to target power grids by enslaving high wattage IoT devices and then switching them on and off to cause line failures, disruption to grid re-starts and increased demand from systems.
- [East Coast of the United States lost access to significant portions of the internet](#) due to one of the largest Distributed Denial of Service (DDoS) attacks to ever hit the internet. The attack occurred in 2016 because of poorly secured IoT devices that were enslaved as part of a global botnet of infected devices.

4.5.2 NSW Cyber Security Policy requirements

While the [NSW Cyber Security Policy](#) focuses on critical systems and data ('crown jewels'), there are cyber security risks to **all** IoT implementations. There are [mandatory requirements](#) within the NSW Cyber Security Policy that cyber teams must understand before implementing an IoT system in NSW.

With regards to crown jewels, the NSW Cyber Security Policy mandates that any systems or data determined by a NSW Government cluster or agency to be a critical asset or crown jewel must be reported to Cyber Security NSW. Risk management of crown jewels is to be covered by either an Information Security Management System (ISMS) or Cyber Security Management System that is compliant with recognised standards such as ISO/IEC 27001 or ISA/IEC 62443.

[ISO27001](#) is the best-known standard from the ISO/IEC 27000 family and provides requirements for an ISMS. An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

IEC62443 has been developed to improve the safety, availability, integrity and confidentiality of components or systems used in industrial automation and control. The

IEC62443 standard includes 4 security assurance levels. The assurance levels define a series of security requirements that need to be met.



Although the NSW Cyber Security Policy is only mandated for NSW Government agencies, Cyber Security NSW recommends that local government councils and state-owned corporations implement requirements within the policy to mitigate cyber security risks.

4.5.3 Challenges in securing IoT

Organisations must be aware of the risks that are introduced by the IoT at all stages of the project development process. The devices that make up an IoT network are well-known in the information security community for being inherently insecure. Challenges in securing IoT devices include:

- IoT devices often lack resources that enable advanced security controls, as they typically have limited processing capacity, memory and power. Manufacturers can be inclined to leave security features out to drive down production costs.
- Often numerous IoT service providers have contributed to the manufacture of IoT devices. These complex supply chains make it difficult to receive software updates. Some components might be discontinued, meaning there is no owner responsible for providing updates.
- The dynamic and evolving nature of IoT means standards and regulation will struggle to keep pace with technology.
- The flow of data from IoT devices can interface to various cloud platforms in both private and public instances which can introduce vulnerabilities.
- Latency issues caused by large amounts of sensors trying to send data to the cloud can, in turn, require an architecture that allows for computing to occur at the edge and not in the cloud. The challenges this creates in enforcing security protocols have been [documented](#).
- It is difficult for security teams to manage risks to and from devices when they are unaware of their existence as these devices are often installed by non-IT personnel, e.g. air conditioning systems, lighting systems, building management systems.

4.5.4 Vulnerabilities in consumer IoT devices

You must ensure the devices you procure do not contain vulnerabilities that are frequently observed in consumer IoT products. The following table summarises the most commonly observed vulnerabilities in consumer IoT devices identified by the Open Web Application Security Project (OWASP).

Top 10 vulnerabilities in consumer IoT devices according to OWASP

Vulnerability	Description
Weak, guessable or hardcoded passwords	<p>Passwords that are not unique can be acquired by an adversary in password lists that are often made publicly available as dumps on paste sites, or for sale on Darknet marketplaces. Password lists can be used by attackers to speed up the process of a brute force attempt on an IoT system.</p> <p> <i>Tip: The Australian Government Information Security Manual recommends that passphrases used as the sole method of authentication should consist of 13 alphabetic characters; or 10 characters with complexity. For further guidance on passwords, visit the Australian Cyber Security Centre website.</i></p>
Insecure network services	<p>Unnecessary or insecure network services running on the device itself, especially those exposed to the Internet, that compromise the confidentiality, integrity/authenticity, or availability of information, or allow unauthorised remote control.</p> <p> <i>Tip: Ensure that only the services required for the device to perform its function are enabled. Services not required must be disabled.</i></p> <p><i>The services that are running on IoT devices should be understood and it is determined if a more secure alternative can be used. For example, if the default service for remote administration is Telnet, consider if the device has enough CPU to handle a more secure alternative such as Secure Shell (SSH) which allows for encryption.</i></p>
Insecure ecosystem interfaces	<p>Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows a compromise of the device or its related components. Common issues include a lack of authentication/authorisation, lacking or weak encryption and a lack of input and output filtering.</p> <p> <i>Tip: Thorough assessment of all components of an IoT system must take place, not only the device and the local network.</i></p>
Lack of secure update mechanisms	<p>Lack of ability to securely update the device. This includes lack of firmware validation on a device, lack of bandwidth to deliver over the air (OTA) updates, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.</p> <p> <i>Tip: It is important to confirm the integrity of software updates with the manufacturer prior to procuring the device.</i></p>
Use of insecure or outdated components	<p>Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customisation of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.</p>

Vulnerability	Description
	 <i>Tip: The Australian Government's Critical Infrastructure Centre provides advice on dealing with risks to supply chain security.</i>
Insufficient privacy protection	<p>Users' personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.</p>  <i>Tip: For guidance on the appropriate collection and use of personal information, see 3.5 Privacy.</i>
Insecure data transfer and storage	<p>Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit or during processing.</p>  <i>Tip: Where possible, personal information must be encrypted with an appropriate algorithm in transit and at rest. Refer to these guidelines for using cryptography.</i>
Lack of device management	<p>Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.</p>  <i>Tip: Consider how devices will be decommissioned at the end of life so that there is no loss of sensitive information. Determine who is responsible for monitoring and responding to security incidents involving IoT systems. Speak to your organisation's ICT and Operational Technology security teams to find a solution to these problems before IoT implementation.</i>
Insecure default settings	<p>Devices or systems shipped with insecure default settings or lacking the ability to make the system more secure by restricting operators from modifying configurations.</p>  <i>Tip: Refer to the Procuring IoT Solutions for advice.</i>
Lack of physical hardening	<p>Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.</p>  <i>Tip: If your system can limit administrative capabilities possible by connecting locally, consider enabling that feature. Disable unused physical ports through the administrative interface.</i>

4.5.5 Cyber security guidance for organisations

a) IoTSF Security Compliance Framework and Checklist

Cyber Security NSW recommends the use of frameworks such as those produced by the IoT Security Foundation (IoTSF) or other applicable standards and guidelines to ensure that minimum controls have been implemented.

For example you can follow the [IoTSF IoT Security Compliance Framework](#) when implementing an IoT solution. This framework has been developed with a [questionnaire that can be used as a checklist](#) to ensure that adequate controls have been implemented to mitigate cyber security risks. Other frameworks for securing IoT systems include:

- [IoTSF Best Practice Guides](#)
- [OWASP IoT Security Guidance](#)
- [ENISA Baseline Security Recommendations for IoT](#)
- [IoTAA Internet of Things Security Guideline](#)
- Data61 IoT Enabled Systems – A Consumer Security Guideline
- [GSMA IoT Security Guidelines](#).
- [Dept. Home Affairs Code of Practice – Securing IOT for Consumers](#)
- IoTAA [Reference Framework](#).

b) Planning for cyber security

You need to consider the following points when planning to procure an IoT solution:

- *Network Segmentation*

Due to the increased amount of cyber security risks that IoT devices introduce, organisations must segment IoT systems from corporate ICT networks and other Industrial and Automated Control Systems.

- *Funding is required for ongoing vulnerability assessments and penetration testing*

Security is not a set and forget activity. As part of all IoT-related business plans and project plans, the budget should be allocated to ensure that there are available funds to develop secure systems as well as for ongoing security tasks such as patching, vulnerability assessments, and incident response. If funding cannot be secured for the lifespan of the system, you should reconsider whether to go ahead with an IoT network.

Vulnerability assessment and penetration testing needs to be an ongoing activity and not a onetime activity that occurs prior to moving into production. Technologies that were considered secure when first implemented can very quickly be deemed insecure with the publication of a new vulnerability.

Cyber security teams do not always have the resources or budget available for penetration testing on every system. You should speak with your organisation's cyber

security team to identify how much funding should be secured for ongoing operational expenditure.

- *Include ICT and Operational Technology (OT) security representatives in the project team and in meetings with potential IoT service providers*

The best way to ensure that security is embedded in your project is to involve security teams from the very beginning. Include security representatives in meetings with service providers when discussing contract terms and project scope to ensure security concerns are addressed in the contract or the features of the IoT solution.

- *Determine who will have sign-off on security deliverables*

Senior security personnel in your organisation must define the security criteria and requirements for an IoT system being implemented. Any assurance process such as the use of the IoT Security Framework must be carried out by a security professional with the authority to report on the suitability of controls and risk profile prior to moving to production.

- *Consider which platform the technology will be run on to ensure that devices can be monitored by security teams*

When procuring IoT systems, organisations should ensure continuous monitoring of events is included as a security feature – for example, Microsoft's [Azure IoT Security](#) and Amazon's [AWS IoT Device Defender](#) are platforms that allow for continuous monitoring of security events. Without alerts in place for security events, it is difficult for security teams to detect, respond or recover from cyber security incidents.

- *Assurance and Certifications of IoT products*

Consider whether IoT products being procured for an IoT project have certification for cyber security which assures the product against common cyber security IoT standards and/or cyber security requirements such as those outlined within this policy.

- *Identification of vulnerabilities and risk management*

Prior to and after being put into production, IoT systems need to be assessed by a penetration tester with recognised industry certifications. A penetration test also needs to be performed in line with any major feature enhancements or configuration changes to a system if it is public-facing.

Recognised industry certifications for penetration testing include Offensive Security Certified Professional (OSCP), Offensive Security Wireless Professional (OSWP), Offensive Security Certified Expert (OSCE), GIAC Penetration Tester (GPEN) and CREST Registered Penetration Tester.

Ongoing vulnerability scanning needs to be performed regardless of changes to IoT systems. Unlike a penetration test, a vulnerability assessment does not involve the exploitation of vulnerabilities for proof of concept. The barrier to entry for performing this task is significantly lower and it can be performed by skilled staff without relevant industry certifications.

Identified vulnerabilities should be assigned to a risk rating and treatment owner. For guidance on establishing risk ratings, refer to an appropriate standard such as [ISO 31000](#).

If vulnerabilities rated as high or extreme are unable to be mitigated, these must be reported to Cyber Security NSW as per mandatory requirement 5.2 of the [NSW Cyber Security Policy](#).

c) **Security by Design**

As with privacy by design, you need to ensure that security by design is embedded in your IoT project. Taking a secure by design approach to software and hardware development minimises cyber security risks and vulnerabilities by embedding security controls into the project from its foundation and reduces project implementation and ongoing costs

You should be adopting a best practice security by design approach throughout the project development lifecycle to ensure security aspects relating to people, processes and technology are considered, with changes implemented to ensure projects are more secure and resilient.

You should consider the following security by design principles throughout the planning, development and implementation of relevant IoT (and broader ICT) projects:

1. **Minimise the attack surface:** restricting access to certain areas by reducing entry points for unauthorised users.
2. **Secure by default:** solving security problems at the root cause rather than treating the symptoms.
3. **Adopt the principle of least privilege:** only the minimum privileges necessary to achieve the desired outcome should be granted to a user, system or process.
4. **Practice defence in depth:** no single security component failure should result in the compromise of an entire environment.
5. **Fail securely and gracefully:** failure of a component must not lead to a lower state of security.
6. **Enforce minimal trust:** validate everything received or entered.
7. **Separation of duties:** no one person should have complete control over critical functions, and security should be enhanced through the division of privileges amongst multiple parties.
8. **Keep security simple:** security designs must be as simple as possible to achieve the required outcomes and minimise the number of errors and vulnerabilities.

9. **Protect sensitive data in transit and at rest:** protect data that is travelling between networks and data that is being stored.
10. **Secure the weakest link:** you are only as secure as your weakest link. Attackers will often focus on gaining access through the weakest link, whether this is a person, vulnerable application or unsecured method of entry.

For more information about security by design please review the Digital.NSW Design standards here or contact Cyber Security NSW.

d) Data considerations for managing cyber security risks

Given the criticality of data to IoT and the significant impact of data breaches, you need to:

- ensure you can log, audit and investigate any issues that may occur
- consider user authorisation, management, and authentication. When different devices connect, ensure that user management and authentication that allow inter-party communication are appropriate
- capture audit data tracking user management and authentication
- ensure authorisation and access is revoked when users leave roles or change organisations or when business or IoT service providers relationships are concluded.

Answering the following questions can help you implement the above strategies:

- What processes require logging?
- Is any autocorrection or overriding of data logged?
- How will logs be managed?
- Who has access to the data in logs?
- How is access to logs managed?
- How is the reliability and accuracy of logs managed?
- Can logs be exported and managed as a record if needed for legal or audit processes?
- What tools are necessary to analyse and interpret logs?

See also [3.5 Privacy](#) for information about managing a privacy breach.

e) Addressing supply chain risk

It is important to assess the security posture of the potential IoT service provider so that supply chains do not become the weak link in securing IoT systems. You can ask prospective IoT service providers questions to help determine if they will protect your supply chain:

- Do they have an Information Security Management System? If so, is it ISO 27001 certified? Can a copy of the Statement of Applicability be provided on request along with a copy of the latest external auditor's report, and the results of recent internal audits?

- Have they implemented the ACSC Essential 8 framework?
- Will they notify your organisation in the event of a security incident?
- Do staff receive security awareness training and if so, how frequently?
- Is there evidence of how cyber security risks are managed for operational technology such as building management systems and other control systems where IoT devices are developed and manufactured?
- Does the IoT service provider have a vulnerability disclosure process/policy?
- Does the IoT service provider have a secure coding policy that must be adhered to by software developers?
- Can the IoT service provider provide references for other organisations that can attest to the service provider's commitment to security? Have the organisations previously suffered a data breach? If so, how was a breach handled?
- What relevant certifications or qualifications do staff possess to ensure quality of work? Can evidence of certifications be provided?

4.6 Data obligations – open, shared and closed data

4.6.1 Open data

Data generated by the government needs to be treated as a public asset and made available as widely as possible. All organisations have the potential to transform customer and service outcomes through the better use of data. Making IoT data from your project open allows other organisations to benefit from, and innovate using, the data you have generated. Making data publicly available in a way that creates access for private and community use can increase transparency, build trust and reduce the number of information requests and costs of responding to these requests.

The [NSW Open Data Policy](#) states that government data should be open by default and protected as required. Further information on making government data open is available from [Data.NSW](#).

You also need to consider the relevant legislation and guidelines when deciding whether to make data open:

- [Government Information \(Public Access\) Act 2009 \(NSW\)](#)
- [Privacy and Personal Information Protection Act 1998 \(NSW\)](#)
- [Health Records and Information Privacy Act 2002 \(NSW\)](#)
- [State Records Act 1998 \(NSW\)](#)
- [NSW Government Information Classification, Labelling and Handling Guidelines](#).

If you make the data or insights generated from your IoT-enabled project open, you must specify the necessary data standards and data quality to enable [interoperability](#).

4.6.2 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 (see Appendix E - also referred to as data sharing principles).

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.

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

4.6.3 Closed data

From an IoT 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.](#)

Case Study – ‘Switch Your Thinking’ in Western Australia

A consortium of councils in Western Australian developed the [Switch Your Thinking project](#) to promote smarter selection of design options in new housing developments. One of the initiatives the councils promoted is a research study on roof colour selection and its impact on house temperatures and therefore energy efficiency.

Using two properties fitted with 36 IoT enabled temperature and humidity sensors on the rooves and inside the house, the councils generated significant longitudinal data sets from regular observations – over 400,000 data points per month.

The data collected from the two properties is open and available online. The project is using this data to raise awareness of the importance of material selection during construction, the impact on building performance and potential costs and savings during operation of the building.

Case study – Using Transport for NSW open data for better customer service

Transport for NSW has installed IoT sensors on buses and trains around Sydney to track vehicle location and capacity and provide real-time information. This data has been made available as open data along with timetable information, and Transport for NSW has encouraged the development of apps to enhance customer experience.

Many of these apps also combine NSW government data with other publicly available data to enhance usability and utility, such as plotting live vehicle feeds on Google maps.

By collecting data and making it open for app developers, Transport for NSW have enabled services that allows citizens to make informed choices about how and when they will travel.

4.7 Technology for IoT

4.7.1 IoT architecture

There are typically three key components to consider when designing your IoT solution architecture:

- *IoT Hub (the Core)*: The IoT component that stores and processes data, and depending on the solution, may also include analytics and management software to control actuators. It may reside in a dedicated data centre or cloud. It may also include device management, that is, control and provisioning. In denser or more complex architectures Hubs may also be considered edge devices. For example, an architecture may have several access point hubs that collect data from sensors, then forward that data to servers (larger hubs).
- *IoT Edge*: The component that responds to or captures data, and depending on the solution, may also include actuators. At a basic level, it may include just a sensor to capture data and send it to the Hub for processing, while an intelligent Edge will include sensors as well as some processing at the Edge for faster response times.
- *Connectivity between Hub and Edge*.

Key components when designing your IoT solution architecture



For more detailed information refer to [the IoTAA: IOT Reference Framework](#) for identifying and positioning elements of the IoT ecosystem. See also the [National Code of Practice](#) which is a voluntary set of measures the Australian Government recommends for industry as the minimum standard for IoT devices.

4.7.2 Requirements in designing your architecture

Your performance requirements, business continuity and back up considerations will help determine how you design your IoT Hub and Edge. Your solution requirements will also help determine the level of intelligence/smartness factor required at the Hub and Edge.

a) Performance requirements

Typical considerations from a performance requirement perspective include:

- Does the IoT service provider's device support direct bi-directional connectivity between the Edge and Hub or is the connectivity passed through the service provider's own data platform between the customer Edge and Hub?
- Does the data captured through the Edge device (e.g. sensor) need to be processed in real-time or is a time lag acceptable?
- Is the fluctuation of device data based on changes in its usage state such that higher bandwidth connectivity is required, or Edge processing needs to be deployed?
- Will the network bandwidth affect data transmission thereby affecting response time? For example, bandwidth may be inadequate to transmit data to the cloud where a video is being processed.
- Is the device uptime and response time critical? For example, in medical and emergency management situations, the response may be required in real-time based on the data intercepted through the occurrence of a particular event. They have a High Intelligent Edge requirement.

b) Business continuity and back up requirements

Typical considerations from a business continuity and back up option perspective include:

- What options exist if the processing ability of the Edge device diminishes or malfunctions? Potentially in such a situation, there may be a requirement for the Edge to be able to intercept data, but instead of processing it at the Edge the device sends it to the Hub for processing.
- Is the loss of connectivity to the cloud is an issue? This may be more of an issue in regional or remote areas than in metropolitan areas.
- Are 'Over the Air' (OTA) updates to Edge devices for security or performance upgrades supported by the IoT solution?

Irrespective of what system architecture is in place or is adopted, it needs to have the following features:

- incorporate privacy, cyber security, data security, and data integrity requirements
- able to receive data from, and send data to, multiple sensor types
- all components of the system need to be able to easily support extensions, upgrades, and inclusion of new modules as they are integrated
- have gateway capabilities and support multiple interfaces to work with different protocols and operation modes. For example, the gateway can be running at the device layer so that the gateway capabilities from the system allow devices to connect through different types of wired or wireless technologies to the system (i.e. ZigBee, Bluetooth or Wi-Fi), or at the network layer, the system

architecture will host the gateway and its capabilities connecting the devices using P2P or VPN protocols.

4.7.3 The importance of interoperability in IoT solutions

a) What is interoperability?

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

To illustrate the concept very simply, lack of interoperability is evident in the inability to charge an Apple iPhone using a Samsung phone charger. If the systems were interoperable you could charge your iPhone using any brand of a phone charger.

Interoperability extends beyond technical interoperability. There should also be agreement on the meaning of data so that applications for one system can easily share and understand data from other systems. Semantic interoperability involves communicating parties or devices having a shared meaning for the data they exchange, using shared data formats and encoding. This is important as incompatible and proprietary data formats create challenges to integrating systems, moving to different services or performing additional data analysis.

b) Benefits of interoperability

Interoperability of IoT solutions can deliver benefits to organisations such as:

- Operational suitability so that the IoT solution can service current or emerging requirements by easily integrating existing 'static' enterprise data with 'real-time' streaming data ingested from IoT devices
- Synergies from integration such as leverage to develop new business processes and outcomes, and avoiding integration issues with legacy systems
- Providing economies of scale such as lower IT management and support overhead, by avoiding different proprietary systems with overlapping functions
- Avoiding vendor lock-in, enabling easier substitution of one IoT service provider for another, ability to inexpensively swap components out for others and to add additional devices from other IoT service providers
- Maintainability of the device and software solution, and access to increased competitiveness around maintenance and expansion costs.

c) How to achieve interoperability

Interoperability is complex as IoT supports various applications across industries and disciplines. Many IoT solutions on the market are proprietary or largely in the

control of IoT service providers, and only support inputs from specific devices. This limits the scope of the solution and potentially leads to vendor lock-in. If one IoT service provider cannot provide your end to end capability, you may need to eventually change over potentially thousands or more of closely tied devices. This is time-consuming and extremely costly.

Full interoperability will not always be possible across products and services. However, you can make choices that will give you a degree of confidence in the interoperability of your IoT solution to the extent it is possible in your circumstances. For example, you can choose IoT solutions that adhere to standards or are an open system, things which are fundamental to interoperability. Another option is that the IoT service provider supports the provision of raw binary data and provides the binary mappings to convert to useable data.

Where full interoperability is not achievable, you need to ensure there is interoperability at the IoT Hub or Core at a minimum so that data can be exchanged and shared.

4.7.4 ‘What technology do I want or need?’ – Things to consider

The IoT market is incredibly diverse. Organisations have a wide selection of IoT solutions to choose from. It is not easy to achieve interoperability.

The recommendations below can help you to increase the prospect of interoperability, procure IoT solutions that meet your current needs, and be ready for new technology and networks as they become available.

A handy checklist for IoT solutions that summarises the recommendations in this chapter is in [Appendix C](#).

a) Questions to determine if an IoT solution is fit for purpose

The IoT Alliance Australia (IoTAA) has published an [Internet of Things Platform Selection Guideline](#) to assist with choosing IoT solutions. The Guideline emphasises the importance of solutions that are fit for purpose. This requires knowing what you want the IoT technology to achieve and what data you want it to collect. It also means understanding the design constraints and core characteristics of prospective solutions.

b) Principles of interoperability

As noted in the [interoperability](#) section, it will not always be possible to achieve full interoperability as IoT is highly heterogenous. Two key principles underpinning interoperability are standards and open systems. Choosing IoT solutions that have these features gives you a better chance of achieving seamless integration of new additions with existing systems over time.

c) Requirements and standards

There are several equipment/device regulatory frameworks in Australia (i.e. telecommunications and radiocommunications). Though the frameworks and the standards which sit under them are not specific to IoT, they may apply to your IoT device depending on how the device operates.

You must ensure that the IoT solution or device you are proposing to install complies with any relevant regulatory requirements. Common regulatory requirements are listed in the following table (this is not an exhaustive list).

Examples of device/equipment regulatory requirements

Regulatory requirements	Link for more information
Radiocommunications standards	Australian Communications and Media Authority (ACMA) - radiocommunications standards
Radiocommunications licences	Australian Communications and Media Authority (ACMA) – radiocommunications licensing
Telecommunications standards	Australian Communications and Media Authority (ACMA) – telecommunications standards
Mobile equipment air interface standards	Australian Communications and Media Authority (ACMA) – Telecommunications (Mobile Equipment Air Interface) Technical Standard
Electrical safety	Electrical Regulatory Authorities Council

IoT systems ideally need to follow the same standards. However, as the IoT market is relatively immature and is everchanging, IoT specific standards are still emerging. IoT service providers and manufacturers can play a part in introducing standardisation to the IoT market by aiming to adhere to appropriate IoT international standards where available which can help promote higher uptake of IoT.

Manufacturers can benefit from making products interoperable as buyers may be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, closed platforms or concerns over vendor lock-in.

The below table lists several ISO international standards which are relevant to IoT architecture and interoperability, though it is not an exhaustive list. These standards have not been adopted by Australia at this stage but, in the interests of standardisation and interoperability within and across organisations, you may find it useful to use the standards.

ISO international standards relevant to IoT

IoT standards	Summary
ISO/IEC 21823-1 Interoperability for IoT systems Part 1	Provides an overview of interoperability as it applies to IoT systems and a framework for interoperability.
IEC 21823-2:2020 Interoperability for IoT systems - Part 2	<p>Specifies a framework and requirements for transport interoperability to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and also among entities within an IoT system. This document specifies:</p> <ul style="list-style-type: none"> • transport interoperability interfaces and requirements between IoT systems • transport interoperability interfaces and requirements within an IoT system.
ISO/IEC 21823.1:2020 IoT Reference architecture	Provides an internationally standardised IoT Reference Architecture using a common vocabulary, reusable designs, and industry best practice.
ISO/IEC 20924 IoT Vocabulary	Provides a definition of IoT along with a set of terms and definitions forming a terminology foundation for IoT.
ISO/IEC TR 22417 IT – IoT use cases	Identifies IoT scenarios and use cases that provide a practical context for considerations on interoperability and standards based on user experience. Also, clarifies where existing standards can be applied and highlights where standardisation work is needed.
ISO/IEC 19637 Sensor network testing framework	<p>Specifies:</p> <ul style="list-style-type: none"> • testing framework for conformance test for heterogeneous sensor networks • generic services between test manager (TMR) and the test agent (TA) in the testing framework, and • guidance for creating a testing platform and enabling the test of different sensor network protocols.
ISO/IEC 20005	Specifies services and interfaces supporting collaborative information processing (CIP) in intelligent sensor networks.

IoT standards	Summary
Services and interfaces supporting collaborative information processing in intelligent sensor networks	
ISO/IEC 29182 series Sensor Network Reference Architecture (SNRA)	Provides guidance to facilitate the design and development of sensor networks, improve interoperability of sensor networks, and make sensor network components plug-and-play, so that it is fairly easy to add/remove sensor nodes to/from an existing sensor network.
ISO/IEC 30128 Generic Sensor Network Application Interface	Specifies the interfaces between the application layers of service providers and sensor network gateways defined in ISO/IEC 29182-5.
ISO/IEC 30144:2020 Internet of things (IoT) - Application of sensor network for wireless gas meters	Specifies intelligent wireless sensor network (iWSN) from the perspectives of iWSN's system infrastructure and communications internal and external to the infrastructure, and technical requirements for iWSN to realize smart electrical power substations.
ISO/IEC 30101 Sensor network and its interfaces for a smart grid system	Characterises the requirements for sensor networks to support smart grid technologies for power generation, distribution, networks, energy storage, load efficiency, control and communications, and associated environmental challenges.
ISO/IEC 30140 series Underwater acoustic sensor network (UWASN)	Provides general requirements, reference architecture and high-level interface guidelines supporting interoperability among UWASNs.

IoT standards	Summary
ISO/IEC 30144:2020 Internet of things (IoT) - Wireless sensor network system supporting electrical power substation	ISO/IEC 30144:2020 (E) specifies intelligent wireless sensor network (iWSN) from the perspectives of iWSN's system infrastructure and communications internal and external to the infrastructure, and technical requirements for iWSN to realize smart electrical power substations.
ISO/IEC 30143:2020 Internet of Things (IoT) - Underwater acoustic sensor network (UWASN) - Application profiles0	ISO/IEC 30143:2020 provides the guidelines for designing and developing new applications in the underwater environment such as fish farming, environment monitoring, harbour security, etc. This document also provides the components required for developing the application; provides instructions for modelling the application with examples; helps the user to understand the communication between the elements in the application for modelling the communication between elements; guides the user with the design process of underwater applications.
ISO/IEC TR 22560:2017 Information technology - Sensor network	This Technical Report describes the concepts, issues, objectives, and requirements for the design of an active air-flow control (AFC) system for commercial aircraft based on a dense deployment of wired and wireless sensor and actuator networks. It focuses on the architecture design, module definition, statement of objectives, scalability analysis, system-level simulation, as well as networking and implementation issues using standardized interfaces and service-oriented middleware architectures.
ISO/IEC TR 30166:2020 Internet of Things (IoT) - Industrial IoT	Describes the following: <ul style="list-style-type: none"> • general Industrial IoT (IIoT) systems and landscapes which outline characteristics, technical aspects and functional as well as non-functional elements of the IIoT structure and a listing of standardizing organisations, consortia and open-source communities with work on all aspects on IIoT • considerations for the future standardization perspective of IIoT including risk analysis, new technologies and identified collaboration
ISO/IEC TR 30164:2020	Describes the common concepts, terminologies, characteristics, use cases and technologies (including data management, coordination, processing, network functionality, heterogeneous computing, security,

IoT standards	Summary
Internet of Things (IoT) - Edge computing	hardware/software optimization) of edge computing for IoT systems applications. This document is also meant to assist in the identification of potential areas for standardization in edge computing for IoT.

d) Open systems

Open systems are fundamental for interoperability. They are systems which can be used by different stakeholders or interfaces between components rather than locked in components via proprietary or obscured interfaces.

You need to choose open technology and/or vendor-agnostic platforms where available to avoid vendor lock-in. For example, this could look like choosing open-source platforms or protocols over proprietary platforms and protocols if available in your location and if the capability is suited to your business or project needs.

Similarly, you may be able to find IoT service providers who try to solve interoperability by offering solutions compatible with proprietary protocols.

e) User Device Detection Capability

It is worth checking if your system architecture provides tools and services for checking the capacity of devices according to the device characteristics required for its application.

By using device-detection techniques and the exchange of communication protocols, this information can be verified at the initial connection attempt. This avoids the user becoming aware of a device's incompatibility only after beginning to use the device.

f) Device management and maintenance

Devices may stand alone or be embedded in a larger product or solution. They may also be complemented by a web application or mobile device app and cloud-based service. You need to consider if you need smartphone or tablet access as not all operating systems used by IoT platform applications to support smartphones or tablets.

You need to consider asset maintenance, such as how (and how often) the device needs to be updated and whether it can be maintained easily.

IoT devices should be able to be managed, monitored and maintained at a component level. This capability should be built-in by the IoT service provider. Consider whether you are prepared to replace a faulty device if one of its faulty components is not able to be replaced, or if it is important to you that just the faulty component can be replaced.

Also, features should be capable of being updated or enhanced, and security vulnerabilities capable of being addressed, through software updates. In other words, firmware should be updateable, and this should be able to be done remotely.

g) Network needs and device connectivity

Users need to consider their network needs in their situation. IoT technology is not a one size fits all approach. Will you be on a public network? Or is it preferable to be part of a private network? If so, communications will be over IP networks and will benefit from improved power and speed.

Network needs will be informed by your priorities and the device itself, and vice versa. Not all devices are well supported by certain network technologies. There are various options for connectivity because IoT applications can differ drastically, meaning varying requirements. Although connectivity technologies are continually being improved, there is a trade-off between range, power consumption, and bandwidth.

There is a vast range of IoT devices on the market working with a range of connectivity technology. At the network edge, IoT devices vary considerably in technical requirements, e.g. wired or wireless, short or long-range, ambient, battery or mains powered, low or high data rates.

IoT is likely to use frequency allocations across the entire spectrum. For example, 4G and 5G standards have made (or will make) specific provisions for dedicated IoT service delivery. Mobile network operators are deploying IoT-specific variants of the 4G standard, such as Narrowband IoT and Category M1 (Cat-M1).

[Appendix D](#) summarises the main IoT network technologies available in NSW.

h) Spatial data requirements for IoT devices

Positioning applications include mobile and stationary devices that communicate regarding their position, time and status. Data collected by such IoT devices can be absorbed into the NSW Digital Twin. To enable this, IoT devices must record certain information as described in [Chapter 6.2 Spatial data requirements](#).

i) Automation and control customisation

IoT solutions generally involve some degree of automation or device control which may or may not be customisable. Automation support may include the use of a business rule engine with pre-defined and/or user customisable rules or machine learning/Artificial Intelligence models developed by business area experts.

Automation may be very simple to extremely complex. You should consider the capabilities of the solution against your automation requirements.

j) APIs and data

An Application Programming Interface (API) provides a software-to-software connection so that two applications can communicate directly without any user intervention. It enables organisations to share and publish data in the most usable forms and to reuse existing technology for a variety of purposes.

A web service is an API that is accessible over the internet through HTTP. Access to third party data should be via HTTPS-based APIs rather than file-based interfaces such as FTP which are often problematic in achieving reliable integration.

Where a system stores or processes data on behalf of a government agency, it should be possible to make that data available via an open API. An open API is publicly available for use by other agencies, the developer community, and the broader public. It is standardised, discoverable, documented, accessible and licensed for reuse.

Whether APIs are delivered 'as a Service', developed in-house or by a third party, APIs should be 'open by default' with minimal restrictions on access. Using an open API increases the opportunities for sharing and reusing open data. The NSW Government API Standard can help agencies to develop, procure and implement API solutions and tools.

APIs developed by third parties or provided as part of a commercial product should also support the release of open data and maintain the safeguards for personal, health or other sensitive information. Take care to understand and determine what functionality is available via the API as typically this is controlled by the service provider.

Providing access to real-time data has implications for the security and capacity of technical infrastructure. Organisations should consider appropriate strategies to mitigate risks, such as using separate servers or networks for data exposed through APIs.

Data services should be provided in the form of two-way stateless API, whereby a set of data is sent to the API and receives return data enhanced with the result of specialist analytics and/or application of expert knowledge. Such services must not retain data provided, nor any derived data without explicit consent.

Datasets or data sources should be described using open standards that facilitate interoperability and data exchange, and persistent identifiers (long-lasting references of URLs).

See the [Digital.NSW](#) website for more information on APIs.

Case study – IoT farming in Bungendore, regional NSW

In 2018 Carwoola Pastoral Company partners with Meat and Livestock Australia (MLA) to create a model farm near Bungendore NSW as an IoT testbed. The model farm consists of four properties with a total footprint of 16,000 acres (6500 ha).

They set up a trial to deploy and test various connectivity and agricultural technology solutions on the farm to understand the benefits of digital farming. The aim was to test, learn and build the foundation for growth at a commercial scale.

The trial used 200 devices and sensors from 22 different service providers to gain practical insights into the current IoT market capability and the benefits it can offer farming. The devices and sensors were for parts of farming deemed to offer the best opportunities for digitisation, including cattle tags, rain gauges, soil probes, pump monitoring, and WHS monitors.

The results of the trial would be used to identify a set of solutions to be deployed at scale, with a Return on Investment model to be built to quantify the benefits from digitising farm operations.

Other lessons from the trial included:

- Poor connectivity on the farm constrained the benefits of the pilot. At best, 3G was available. To overcome this, at least one IoT communications network was deployed as part of the trial to test and compare the various options, their pricing, and support models. Across the four properties, there are now four LoRaWAN gateways, Sigfox gateways, satellite IoT and on-farm Wi-Fi. With mixed topography, the technology mix has been beneficial in providing greater coverage and servicing a diverse range of use cases.
- There was a lack of reporting interoperability resulting from having so many suppliers and sensors. There was no integrated reporting dashboard which meant multiple interfaces for data and dashboards.
- Solutions were tested and continuously assessed for their suitability and robustness, creating a feedback loop for the AgTech industry to refine and create fit-for-purpose solutions.

Case study – IoT network connectivity and cotton farming in regional NSW

Goanna Ag is partnering with the National Narrowband Network Co (NNNCo) to roll out the rural LoRaWAN network in regional NSW for smarter irrigation in cotton. The network is aimed at enabling IoT powered irrigation solutions for the cotton industry with planned deployments of nearly 100 gateways in NSW and Queensland along with 2000 sensors across cotton farms in 2019. The sensors include soil moisture probes, rain gauges, weather stations, and water and fuel tank monitors and satellite imagery.

Cotton is a resource-intensive crop and by tapping into the IoT network, farmers can make data-driven decisions to accurately schedule and irrigate cotton farms. The program will provide granular real-time data on a range of measures and enable remote management to monitor sites and send commands from the network back down to a sensor or actuator.

LoRaWAN has been proven to be successful in Australia. Having a Low-Powered Wireless Area Network (LPWAN) enables connectivity in a regional location which usually has poor connectivity. The network can send small packets of essential data using very low power and at a low cost.

Having a LoRaWAN network backbone builds rural connectivity and gives farmers the flexibility to adopt different technologies quickly and easily. Any compliant LoRaWAN sensor will be able to connect to the network.

4.8 Assurance

4.8.1 Why is assurance important for IoT?

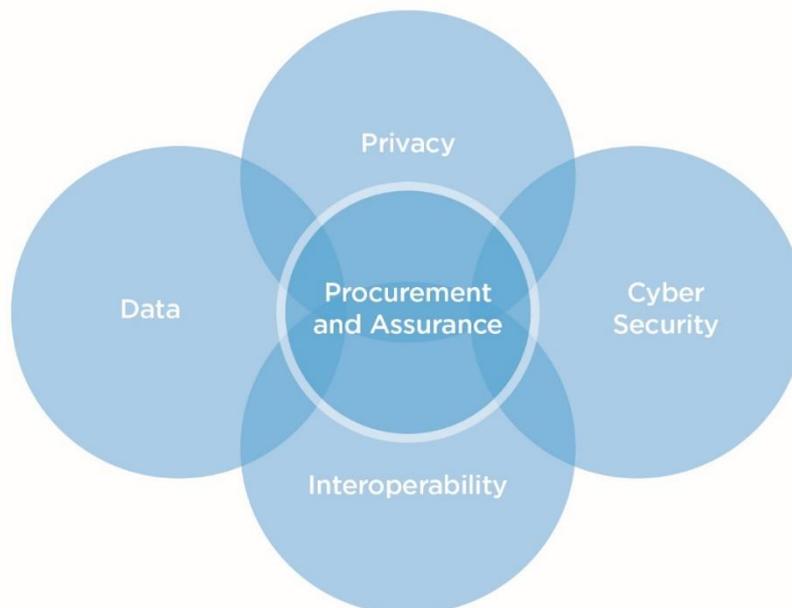
Assurance is the process of providing independent confidence for projects. Assurance involves regularly examining a project against an approved business plan and what it was intended to do, or service needs it was intended to meet.

An assurance process can increase confidence in the project benefits and reduce the likelihood of investing in IoT solutions that are not fit for purpose, present unmanageable risks, do not deliver benefits or are not interoperable with existing or future technologies.

Assurance is important for IoT-enabled projects because the technology is new and brings together numerous areas of expertise. Connectivity is at the core of IoT which means IoT-enabled projects are more susceptible to a wider range of risks—risks that only increase when we connect IoT solutions to bigger networks.

The following diagram demonstrates the overlap between different areas of expertise and therefore risks. See [Chapter 3.4 Risks and obligations](#) for further discussion of risks with IoT and mitigation techniques.

Intersection of IoT-related risks with assurance



4.8.2 What assurance does my project need?

You must consider what assurance processes may apply to your IoT-enabled project. Some degree of assurance should apply to all projects. Assurance may be provided via:

- Gateway Reviews for NSW Government
- internal assurance at an organisational level.

a) Gateway Reviews for NSW Government agencies

The [NSW Gateway Policy](#) establishes three assurance frameworks. Each assurance framework is managed by a Gateway Coordination Agency (GCA) to deliver [Gateway Reviews](#). NSW Treasury is the policy owner responsible for the overall NSW Gateway Policy.

Under a Gateway Review, reviews are conducted by independent experts at up to seven decision points (gates). The project's key stakeholders are interviewed, and key documents are examined. Gateway Reviews are not audits but rather confidence reviews, providing an independent view of the project. They aim to prepare the project for success.

No assurance framework specialises in IoT, but IoT may still fall under an assurance framework. Use the decision tree at [Attachment A of the NSW Gateway Policy](#) to determine what assurance framework your project may fall under. If you are unsure of which assurance framework your project may fall under, contact the [Treasury Gateway team](#) or the most relevant GCA.

If your IoT-enabled projects meet the requirements of an assurance framework, you must register it with the relevant GCA.

The following table sets out the scope and threshold for the three assurance frameworks.

Three assurance frameworks for NSW Government

Assurance framework and GCA	Projects covered by the assurance framework	Project value (\$)	Example of IoT-enabled projects
ICT Assurance Framework NSW Department of Customer Service	<ul style="list-style-type: none"> Information and Communications Technology (ICT) Programs directed by Cabinet Programs nominated by NSW Treasury or self-nominated by the NSW Government agency. 	\$10 million or higher (unless the project is of or strategic importance/ high risk)	Mobile pathology machines to test a patient's blood at the point of care.
Infrastructure Investment Assurance Framework Infrastructure NSW	<ul style="list-style-type: none"> Infrastructure Equipment Property Development Operational Technology Programs directed by Cabinet Programs nominated by NSW Treasury or self-nominated by the NSW Government agency. 	\$10 million or higher	Installation of sensors to monitor traffic volumes, types of vehicles and the condition of the road
Recurrent Expenditure Assurance Framework NSW Treasury	<ul style="list-style-type: none"> Recurrent expenditure projects and programs (excluding predominantly capital infrastructure and ICT investment) Programs directed by Cabinet Programs nominated by NSW Treasury or self-nominated by the agency. 	Greater than or equal to \$100 million over four years, or greater than or equal to \$50 million per annum.	Cleaning contracts that use IoT devices to remotely monitor bathroom cleaning needs.

b) Internal assurance

You need to engage in some form of internal assurance to monitor the ongoing viability of your project regardless of whether your project meets the threshold for a Gateway Review (or if you are a local council). The Gateway Assurance process is not a substitute for an internal assurance process. Check within your organisation what internal assurance processes exist.

Take a risk-based approach to ensure the scale of assurance is proportionate to the project. For example, low risk/value projects will have a less onerous assurance process involving fewer touchpoints in the project lifecycle than a high risk/value project.

Remember that assurance can be carried out by anyone independent of the project. This may be someone within your organisation who is not involved in the project, by a partner agency or local council (this can assist with building capability across the sector) or by another external person with relevant expertise.



Tip: Each module in this policy guidance begins with a checklist of 'key takeaways' (for modules 1 and 2) or 'best practice considerations' (for modules 3 to 8). Be sure to read these checklists and incorporate them into your project.

5. Making the Case

Best practice considerations at this stage in a project

- Has the business case accurately budgeted for training, handover and operational readiness tasks?
- Is the business base realistic, clear and unambiguous in detailing the outcomes, scope, scale and requirements of the project?
- What are the stakeholder issues that may prevent the project from maximising benefit and optimising cost and how will these be addressed through the business case?
- Has the availability of funding for the whole of the project been confirmed? Is the project's whole of life funding affordable and supported by key stakeholders?
- Has the appropriate financial and cost-benefit analysis of the project been completed?
- Have you considered the long-term as well as short-term benefits of your project?

5.1 Business case

Defining your problem and drafting a business case is key to the success of your IoT-enabled project. This chapter provides guidance on how to make the case for IoT and how to identify your objectives, risks, benefits, costs, and stakeholders.

5.1.1 What is a business case?

A business case is a document providing justification for a proposed investment or policy decision. For the NSW Government, they are an important tool to inform evidence-based investment decisions by government.

A business case generally contains analyses of the costs, benefits, risks, and assumptions associated with various investment and policy options to achieve policy or program outcomes.

NSW Treasury's [NSW Government Business Case Guidelines](#) indicate five main components of a business case:

- 1) *A case for change*: What is the business need and how does it fit strategically?
- 2) *Cost-benefit analysis*: What are the options to address an objective and do they maximise social welfare and deliver value for money?
- 3) *Financial analysis*: Is the intervention financially feasible? Is it affordable?
- 4) *Commercial analysis*: Is there capacity and capability (within your organisation and in the market) to procure, supply and maintain the service level proposed?
- 5) *Management analysis*: Can the intervention be delivered?

A business case can be a short document of a few pages that contains information on objectives, costs, benefits, risks, and stakeholders. Or, it can be a longer, more detailed analysis.

The length and detail of your business case can be based on the:

- complexity of your project
- size of the funding request
- potential risks
- availability of evidence
- contributors involved in the proposal development e.g. one cluster or cross-cluster
- number and type of stakeholders impacted e.g. internal or external
- criticality of service, e.g. substantial impact to existing service delivery processes
- strategic objectives it needs to align with
- degree of innovation and time involved in the realisation of benefits.

5.1.2 Why should a business case be prepared?

IoT is an emerging technology. This means the associated costs, benefits, risks, and opportunities are not yet easily articulated or forecast. A robust business case provides decision-makers with the assurance that your IoT-enabled project provides value for money, risks have been considered and mitigated, project management is sound, and the project is consistent with government priorities and objectives.

Business cases are prepared for different reasons:

- to inform an investment or regulatory decision
- to demonstrate that adequate due diligence and thinking was undertaken
- to obtain approval including funding.



Tip: NSW Government agencies will soon be able to apply for investment from the new Digital Restart Fund announced as part of the NSW Budget 2019-20. The Digital Restart Fund will be a \$100 million fund to accelerate whole of government digital transformation projects over the next two years. You may be able to seek funding for new IoT-enabled projects.

5.1.3 When should a business case be prepared?

Business cases may need to be submitted to NSW Treasury as part of the annual outcome-based budget process, or as part of the Gateway Review process. [Chapter 3.9 Assurance](#) provides information on the Gateway Review process and when it applies.

It is good practice to prepare business cases for proposed investments as part of your organisation's internal decision-making process. Discuss the requirements for the project with your organisation's Project Management Office.

5.1.4 How to prepare a business case

There are three main stages of business case development:

- Stage 0 – Problem Definition
- Stage 1 – Strategic Business Case
- Stage 2 – Detailed Business Case

The following table summarises what is involved in the three stages. For more detailed information, including on how to complete the activities and analyses in each stage, refer to the [NSW Government Business Case Guidelines](#).

Three stages of a business case

	Stage 0: Problem Definition	Stage 1: Strategic Business Case (SBC)	Stage 2: Detailed Business Case (DBC)
Overview	<ul style="list-style-type: none"> This stage outlines the need, opportunity or the case for change. It is a short, high-level document based on the evidence available at the time. 	<ul style="list-style-type: none"> This stage provides the decision-makers with an indication of whether there are beneficial options to address the objectives. The evidence expected at this stage is preliminary. 	<ul style="list-style-type: none"> This stage builds on the analysis undertaken in Stage 1 to select a preferred option. It also includes the commercial and management arrangements for the procurement and delivery of the project.
Purpose	<ul style="list-style-type: none"> Needs analysis and confirmation. Seek approval to proceed with the development of a Strategic Business Case. Engage with stakeholders during this stage, including users of the service. 	<ul style="list-style-type: none"> Option(s) analysis. Reconfirm the need for action and case for change. Consider value for money and feasibility. Seek approval to proceed with the development of Detailed Business Case. 	<ul style="list-style-type: none"> Option selection. More comprehensive analysis. Develop commercial plans. Develop management arrangements.
Approach	<ul style="list-style-type: none"> Identify the need for government intervention and make the case for change. Identify the problem, benefits, strategic response, costs, risks, and stakeholders. 	<ul style="list-style-type: none"> Confirm the case for change. Identify and screen options that meet the intervention objectives based on a high-level analysis. 	<ul style="list-style-type: none"> Confirm the way forward. Shortlist options. Select the preferred option based on a thorough analysis. Assess commercial and management aspects for the selected option.
Output	<ul style="list-style-type: none"> Progress with Strategic Business Case. You may need 	<ul style="list-style-type: none"> Confirm way forward. 	<ul style="list-style-type: none"> Confirm the preferred option.

	Stage 0: Problem Definition	Stage 1: Strategic Business Case (SBC)	Stage 2: Detailed Business Case (DBC)
	<p>approval from key stakeholders to proceed past this stage.</p> <ul style="list-style-type: none"> • If necessary, seek funding approval for the next stage based on the output of this stage. 	<ul style="list-style-type: none"> • Progress with Detailed Business Case. • If necessary, seek funding approval for the next stage based on the output of this stage. 	
Relevance for IoT-enabled projects	<ul style="list-style-type: none"> • This stage is to be completed when you are still analysing the problem or benefit you are trying to address – before you have identified an IoT solution as your preferred option. 	<ul style="list-style-type: none"> • At this stage, you will identify an IoT solution as a potential option, among other possible options. You may still be comparing IoT solutions with a non-IoT solution. See Chapter 2.1 Is IoT the appropriate tool to use? for help with this analysis. 	<ul style="list-style-type: none"> • At this stage, you analyse whether an identified IoT solution is the best option. Depending on the complexity of your project and the information available, your DBC may be quite short.

The three stages of a business case include activities aligned to different stages in the business case development process. You may or may not be required to complete every activity – this depends on the complexity and size of your IoT-enabled project. The below table outlines the key activities that need to be completed for a best-practice approach.



Tip: For complex projects, develop your business case in stages (i.e. problem definition, strategic business case, detailed business case) and seek approval at each stage. For smaller, less complex projects where a detailed and lengthy business case and analysis is not required, you can develop the business case in one go and seek approval for the entire business case.

Activities throughout the three stages of a business case

Type of activities involved	Stage 0: Problem definition	Stage 1: Strategic business case	Stage 2: Detailed business case
Case for change	<ol style="list-style-type: none"> 1. Define business needs/challenges or opportunities. 2. Business case objective(s). 3. State outcomes/ outcome indicators. 4. Define benefits and define project KPIs. 5. Identify relevant stakeholders. 6. Identify strategic responses /interventions to achieve objectives. 7. High-level cost estimates for the responses identified. 	<ol style="list-style-type: none"> 8. Review the case for change. 	<ol style="list-style-type: none"> 13. Confirm the case for change.
Cost-benefit Analysis (CBA)		<ol style="list-style-type: none"> 9. Identify and assess the long list of options (option appraisal). 10. Assess and narrow down your options (conduct a stage 1 CBA – see Chapter 4.2 Cost-benefit analysis for guidance). 	<ol style="list-style-type: none"> 14. Revisit the CBA and confirm the shortlist of options. 15. Select preferred option – conduct Stage 2/full CBA on shortlist of options.
Financial analysis		<ol style="list-style-type: none"> 11. Assess and narrow down your options (prepare a 	<ol style="list-style-type: none"> 16. Revisit the FAP and FIS to confirm the shortlist of options.

Type of activities involved	Stage 0: Problem definition	Stage 1: Strategic business case	Stage 2: Detailed business case
		Financial Appraisal Profile (FAP)). 12. Assess and narrow down your options (prepare a Financial Impact Statement (FIS)).	17. Select the preferred option – conduct Stage 2/full FAP on shortlist of options. 18. Prepare a FIS on shortlist of options to define the impact on costs and savings.
Commercial analysis			19. Develop a procurement strategy. 20. Specify technical requirements. 21. Identify contractual issues.
Management analysis			22. Establish governance arrangements. 23. Establish a project management strategy, framework, and plan. 24. Establish a change management strategy and plan – see Chapter 6.1 Change management for guidance. 25. Develop a benefits plan and register. 26. Establish a risk management strategy, framework, and plan – see Chapter 3.4 Risks and obligations for guidance. 27. Establish a post-implementation evaluation plan – see Chapter 8.1 Evaluation for guidance.

Update and revise the business case as necessary if further information becomes available. This will assist when evaluating your IoT-enabled project at a later stage, which is particularly important if you are making one of the first cases for IoT in your organisation/team and need to demonstrate its benefits.

For assistance completing your business case, see the below resources or speak to your organisation's Project Management Office.

5.1.5 Additional resources

- [The NSW Government Business Case Guidelines \(TPP18-06\)](#) establish a best practice, clear and consistent approach to preparing a business case.
- [The NSW Treasury business cases webpage](#) provides templates for the three business case stages outlined in this chapter and in the NSW Government Business Case Guidelines.
- If your IoT-enabled project is classified as an infrastructure project, the [Infrastructure NSW Business Case Toolkit](#) can assist with developing a business case.

5.2 Cost-benefit analysis

This chapter explains how to ensure that IoT-specific costs and benefits are considered and incorporated into your business case.

5.2.1 What is a cost-benefit analysis?

Cost-benefit analysis (CBA) is a decision-making tool that estimates the economic, social and environmental costs and benefits of a project or program in monetary terms. It is an important element of a project's business case.

The aim of a CBA is to measure the full impact of any government decision or action on the affected community. For NSW Government projects, a CBA should focus primarily on impacts to the NSW community – households, businesses, workers and/or governments. Ultimately, a CBA reports on whether the benefits of a proposal are likely to exceed the costs and provide a net social benefit.

5.2.2 How to conduct a cost-benefit analysis

Your organisation's Project Management Office (or relevant team) can help you with a CBA.

A key resource is the [NSW Government Guide to Cost-Benefit Analysis \(TPP 17-03\)](#) is a step-by-step guide to CBA.

Another useful resource is the [NSW Government Benefits Realisation Management Framework](#). It was developed to assist NSW Government agencies to identify, plan, manage and evaluate the intended benefits of a project.

5.2.3 Considering costs and benefits for IoT-enabled projects

a) Determining costs and benefits for IoT-enabled projects is complex

Conducting a CBA for an IoT-enabled project is often less straightforward than for typical government investments. There are various reasons for this:

- A single IoT solution usually consists of diverse components integrated into a complex system. For example, a solution will have various non-technology components as well as different technology components like sensors, actuators, networks, cloud data centres, and data management systems (which all have their own features and requirements around energy consumption, maintenance, security testing). Understanding the cost structure of each of these components can be complex.
- A “as a service” (i.e. annuity based) business model is often the approach favoured by IoT service providers, introducing an ongoing expenditure that needs to be considered.
- IoT components may have various owners and/or operators, each of whom incurs a different cost and derives a different benefit from the whole system
- IoT-generated data that is shared often contains indirect value to other stakeholders that is unforeseeable to the project owner
- There are risks and opportunities associated with IoT that may have intangible costs or benefits (e.g. environmental or customer benefits with no immediate cost-benefit return).

b) Considerations in analysing costs and benefits for IoT

The complex nature of IoT means it can be difficult to forecast and calculate costs and benefits with confidence. All costs and benefits should still be described and captured, along with any assumptions underlying how the calculations were made.

Additional expertise may be required to analyse your project’s costs and benefits to ensure it is valued accurately, taking into account IoT-specific considerations. Some of these considerations are outlined below:

- One of the primary benefits of IoT, even for the simplest of applications, is the wealth of data that can be captured. The physical core of IoT is devices and connectivity, but the resulting data, analytics and actionable insights are how organisations derive value. The ability to share the data and insights across government will perpetuate the return on investment.
- Not all data is equally valuable. For example, data used for optimisation and prediction have more potential uses and is therefore generally more valuable than data used for specific purposes such as anomaly detection and control.
- Your IoT solution will incur ongoing costs for data access, storage, processing, and analytics.

- Data ownership needs to be considered (i.e. who has access to the data and may use it for analysis and further processing).
- Keeping your devices and data secure will require regular testing and investments.
- It is important to understand the technology life to cost in upgrades. There is an interdependency with how long the solution is required to be maintained. There are also ongoing operating costs for your devices include power supply, connectivity, maintenance (e.g. batteries replacement) and updating.
- There are ongoing costs for cyber security including for regular penetration testing.
- Value from an IoT-enabled project can be maximised if interoperability between IoT systems is increased. See [Chapter 3.8 Technology for IoT](#) for information on interoperability.
- It may be costly to retrofit IoT to your existing asset base or infrastructure. However, experimenting with a retrofitted device may teach you how to design proven IoT solutions in new assets and infrastructure.
- Consulting with third parties may be required if your project team does not have the capabilities to plan, implement and manage your IoT solution.
- Consideration can be given to risk/benefit-sharing approach between your organisation and the IoT service provider(s). That is an approach where the potential savings is shared between your organisation and the IoT service provider(s). This mechanism can be used to lower initial outlay of capital and ensure IoT service providers stay engaged in ensuring business value is delivered through the project.
- As IoT and its many possible implementation variations are still an emerging technology, IoT service providers are often interested in establishing credible case studies. This can be monetised and used to establish a strong partnership with IoT service providers who will have a vested interest in delivering true business value.

Case Study – Sydney Water’s use of IoT for the wastewater network

Sydney Water is using IoT to detect sewer blockages and predict overflows so that it can detect issues in the wastewater network before customers and the environment are impacted. A high priority is the ability to detect sewerage blockages in real-time, allowing crews to respond faster. The technology also presents the opportunity to move to predictive maintenance.

Sydney Water has explored technologies such as level switches, ultrasonic level sensors and sewer flow sensors. They have been deployed across 280 devices of 15 different models (both off the shelf models and models developed in-house). Sensors are spatially enabled so that Sydney Water knows where the sensors are, and they have an alarm panel to advise when a blockage occurs in the sewer network.

The sensors are connected to a range of networks: Sigfox, LoRa, Taggle, and Telstra NB-IoT networks as well as a SCADA system. A Telstra IoT platform ingests the data collected which then plugs into Microsoft Azure for data storage and processing before it is presented in data analysis applications.

The benefits realised from this work include:

- 20 sewer blockages detected in time to be cleared by crews
- high impact overflows averted with 4,700 properties upstream
- potential alternative to preventive maintenance
- breakdown maintenance effectiveness monitored.

6. Procure

Best practice considerations at this stage in a project

- Are you clear on the procurement outcome you want to achieve and the problem you are trying to solve?
- Do you understand your end user needs? How are these needs reflected in the procurement strategy, specifications and evaluation?
- Do you understand your technology requirements (i.e. bandwidth) and any restrictions (i.e. network availability)?
- Have you drawn on the necessary expertise in your organisation (or externally) to:
 - develop your specifications and procurement strategy
 - design evaluation criteria
 - evaluate proposals (i.e. on evaluation panel)?
- Do you understand the capability of existing and potential suppliers? Are they ready, willing and able to respond to specifications?
- What is the planned approach to market? Why is it the most appropriate means to achieve the desired procurement outcome?
- Have you identified the procurement risks? How are these risks managed or mitigated through the procurement strategy, approach to market, tender documentation and evaluation?
- Have procurement risks been allocated to the party best able to manage the risk, and how is this reflected in the contract?
- Do your procurement specifications clearly state your data needs, and if you own the data? Do your procurement specifications clearly state your security parameters?
- How are you ensuring that your IoT solution is interoperable?
- Who is responsible for maintenance and upkeep of the IoT solution and supporting systems, and how is this reflected in the procurement specifications?
- How does your contract deal with re-competition? Is there an exit strategy to ensure that you are not locked into a service provider and/or solution?
- Is the proposed IoT solution scalable? If so, how has this been reflected in the contract?

6.1 Procuring IoT solutions

6.1.1 Procuring IoT goods and services

The [NSW Procurement Policy Framework](#) defines procurement (or sourcing) as the end-to-end buying process from needs identification to market engagement, contracting and placing orders, managing contracts and service provider relationships, and disposing of government assets.

The broad application of IoT, the relative immaturity of the IoT service provider market, and the lack of maturity and capability on the buyer side can make procuring IoT solutions challenging.

6.1.2 Procurement landscape

NSW Government agencies must comply with [Part 11 of the Public Works and Procurement Act 1912 \(NSW\)](#) and the [NSW Procurement Board's](#) policies and directions. The NSW Procurement Policy Framework sets out government procurement objectives and the Procurement Board's mandatory requirements. There are no existing NSW Government prequalification schemes or panel arrangements specialising in IoT technology.

[Procurement Board Direction 2019-05 Enforceable Procurement Provisions](#) sets out the obligations for NSW Government agencies arising from free trade and other international agreements. These obligations can be legally enforced by suppliers, including seeking an injunction or compensation in the Supreme Court for an alleged breach. For procurements over the thresholds in the Direction, agencies must ensure their procurement process complies with these obligations.

Local councils are not governed by the NSW Procurement Board and are therefore not required to follow the NSW Procurement Policy Framework or the Procurement Board Directions.

Local councils must comply with [section 55 of the Local Government Act 1993 \(NSW\)](#) and [Local Government \(General\) Regulation 2005 \(NSW\)](#). This requires councils to tender for contracts over \$250,000 (including GST) unless they procure from a NSW Government panel or NSW Government prequalification scheme (a list of NSW Government panels and prequalification schemes can be found [here](#)).

6.1.3 Contacts for procurement

These resources can help you with your procurement journey:

- NSW Government agencies can contact your cluster's Chief Procurement Officer for tailored advice and information on the procurement processes and resources available in your agency.

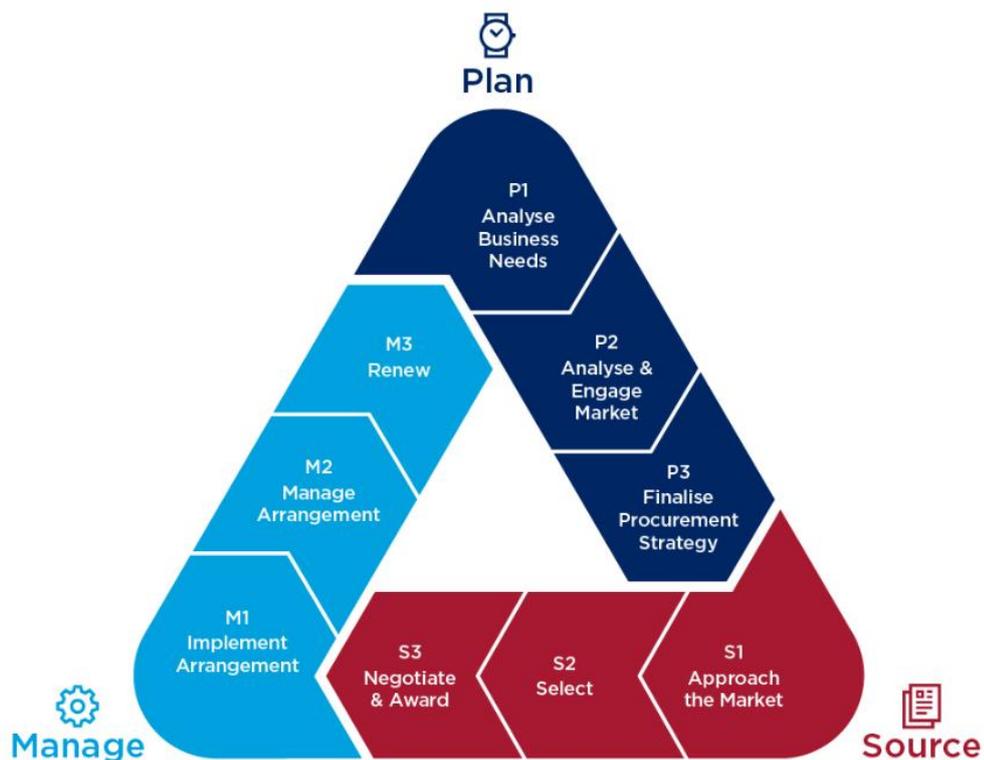
- [buy.nsw](#) is your one-stop shop for all NSW Government procurement information. It is where all whole of government procurement policy, guidance and training is published.
- The [NSW Procurement Service Centre](#) can provide general advice on whole of government procurement policy, Board Directions, whole of government contracts and prequalification schemes.
- Local councils can contact your internal procurement teams of Regional Organisations of Councils (ROCs) for procurement support.

6.1.4 How do I procure?

a) What is a best practice procurement process?

Procurement involves three broad stages – plan, source, manage. Use the [NSW Procurement approach](#) for a step-by-step guide to best practice procurement.

The three stages of procurement



b) Managing challenges in the procurement process

Key challenges in the procurement process for IoT are:

- *You may need to procure a combination of hardware, software, and services*

Ensure your procurement process considers the whole of life costs, including any external support needed to maintain the IoT solution or service. For

example, the IoT service provider may collect, store and analyse the data captured for your organisation.

- *Ensuring your procurement strategy supports industry participation*

IoT service providers must be ready and able to meet your procurement needs. Early industry engagement activities can help you to understand IoT service provider capability prior to releasing a tender (see the [nine key steps of industry engagement](#)). You also need to select the best approach to market for your procurement needs (see the [Market Approaches Guide](#)).

- *Leveraging the right skillset to procure the right IoT solution*

IoT relies on many technical disciplines (e.g. cyber security, privacy, enterprise architecture, IT, data). You need to make sure these technical experts contribute to the development of the procurement specifications and evaluation of responses.

- *Optimising IoT service provider performance to realise ongoing value for money*

A good working relationship with the successful IoT service provider is vital to deriving value over the life of the contract and achieving the agreed outcome. IoT technology is rapidly changing so you may need to adapt to continue to see the value. You cannot 'set and forget'. See the NSW Procurement Approach for guidance on how to manage the IoT service providers.

6.1.5 What to do if the perfect solution does not exist

The rapidly evolving nature of IoT means that the Procurement Innovation Stream can be used to pilot new solutions. Information on the Procurement Innovation Stream can be found in the [NSW Government Small and Medium Enterprise and Regional Procurement Policy](#) (for goods and services) and [PBD-2019-03-Access to government construction procurement opportunities by small and medium-sized enterprises](#) (construction).

Local councils cannot use the Innovation Stream. It is recommended that councils work with industry to design specifications that are outcomes-focused and meet the technical requirements.

6.1.6 Designing specifications

The specifications you release to market need to clearly state the outcome you want and the boundaries for IoT service providers to respond to. This table sets out considerations when developing specifications for projects involving IoT.

Considerations when building specifications for IoT-enabled projects

Consideration	Description
Focus on outcomes and success criteria	<p>Being clear about your desired outcome and success criteria creates opportunities to achieve the same outcome through different means. For example, if you want to improve public safety, IoT service providers can provide different solutions including smart lighting, GPS monitoring, and CCTV cameras.</p> <p>Prescriptive specifications are used when you clearly understand your needs and the product requirements, for example, a decision has been made to procure smart lighting. This narrows the diversity in IoT service provider responses.</p>
Network needs	You need to think about what sort of network connectivity is required. For example, will your IoT device need to be accessible through public internet or a private network? See Chapter 3.8 Technology for IoT for network options.
Asset maintenance, asset onboarding, and management	<p>Understanding how a device will be installed, how often and how easily it can be updated, and the availability of replacement parts can help your future-proof your IoT solution.</p> <p>Also, think about maintenance requirements for the broader IoT ecosystem (i.e. how do the maintenance needs of your IoT solution align with other IoT devices used by your organisation). See also Chapter 3.8 Technology for IoT and Chapter 7.3 Device and data maintenance.</p>
Designing your IoT architecture	To design your IoT Hub and Edge, you need to consider your requirements around performance, business continuity and back up. See Chapter 3.8 Technology for IoT for guidance.
Sensor positioning data	Sensors that will (or have the potential to) feed into the NSW Digital Twin must record the device location and a time and data stamp in accordance with the requirements set out in Chapter 6.2 Spatial data requirements chapter .
Scalability	Consider if the current scope/use of the IoT solution may be expanded in future. For example, if it is a pilot, it may be used in other locations or across NSW if successful.
Interoperability	Interoperability is complex as IoT supports many applications across different industries and disciplines. You need to understand the existing technology systems in place that may affect the IoT solution's ability to achieve the

Consideration	Description
	desired outcome. Your IT department is the best source of information. See also Chapter 3.8 Technology for IoT for more on interoperability.
Open source versus proprietary systems	Open-source systems are fundamental to interoperability. You should choose open technology where available to avoid vendor lock-in. Similarly, you may be able to find IoT service providers who try to solve interoperability by offering solutions compatible with proprietary protocols.
Privacy and personal information	Do not collect personal information unless absolutely required. Data collected using sensor networks may be personal information if it is about an identified person or can 'reasonably' be linked to an identified person. See also Chapter 3.5 Privacy .
Relevant standards	Investigate if there are any standards instruments that are applicable. These may be international, national, or specific to your organisation. Chapter 3.8 Technology for IoT lists standards related to IoT, devices, and equipment.
Cyber security	IoT devices are inherently insecure. You should embed cyber-related risks into your procurement business case. See Chapter 3.6 Cyber security for a list of vulnerabilities.
Data requirements	<p>Specifications should include:</p> <ul style="list-style-type: none"> • data requirements, including adherence to data standards and data quality requirements • privacy and information security requirements, including adherence to legislation and government policy • data breach and security incident notification and management processes • data quality requirements • data ownership and rights, including for data assets generated from multiple sources • data retention and disposal requirements, including when the contract ceases or is terminated • data storage requirements, including data sovereignty

Consideration	Description
	<ul style="list-style-type: none"> legislative compliance requirements, including the Privacy and Personal Information Protection Act 1998 (NSW), Health Records and Information Privacy Act 2002 (NSW), Government Information (Public Access) Act 2009 (NSW), State Records Act 1998 (NSW). <p>See also Chapter 5.2 Data considerations for contracting.</p>
Indemnities	<p>Indemnities support insurances in managing contract risks and should be appropriate to the size and risk of the investment. NSW Government agencies are required to cap indemnity given by a service provider, which is determined based on the goods or services involved. More information is available at https://buy.nsw.gov.au.</p>
Insurance	<p>You need to consider:</p> <ul style="list-style-type: none"> the level of public liability required (taking into account the risk profile of the procurement and products or services) if professional and/or product insurance is required, and if so, what is the appropriate level. <p>Unnecessarily onerous insurance requirements will increase the cost of the procurement. More information is available at https://buy.nsw.gov.au.</p>
Change management	<p>Consider the costs and impacts of transitioning from the existing state to a new system, product and IoT service provider.</p>

6.1.7 Procurement risks

Identification, assessment, and treatment of risks are integral to the procurement process. By identifying potential risks during the planning stage, you can formulate a plan to mitigate them. The effort expended in managing risks in a procurement process should be consistent with the estimated cost, complexity and nature of the procurement.

When identifying the risks and potential treatments to mitigate them, people with relevant expertise should be consulted (for example, privacy, information management, cyber security experts).

It is the nature of risk and risk management that, sometimes, unexpected problems occur. When this happens, it is important that the reasons and circumstances are identified, documented and taken into account with future risk analyses including updating guidance documents. Remember to document your risks in a [Procurement Risk Register](#).

The table below sets out common procurement risks and avoidance techniques. It is not an exhaustive list. More information on risks throughout the IoT user journey is available in the [Risks and obligations chapter](#).

Common risks in procurement involving IoT goods and services

Procurement risk	How to avoid it
<p>Insufficient lead-time resulting in inadequate responses from and higher prices from prospective IoT service providers</p>	<ul style="list-style-type: none"> • Involve procurement officers in the project planning phase. • The NSW Procurement Board Industry Engagement Guide provides advice on planning industry engagement activities and how to incorporate the outputs and outcomes into the formal procurement process.
<p>Inadequate or unclear specifications that:</p> <ul style="list-style-type: none"> • result in responses which are insufficient/ do not meet your needs/are difficult to evaluate • create the possibility that evaluation will not meet probity/ audit scrutiny 	<ul style="list-style-type: none"> • Seek advice from procurement officers or other teams or organisations that have experienced similar issues. • Have a clear understanding of the problem you are trying to solve/outcome you want to achieve and your success criteria. • Run a multi-stage tender process where you: <ul style="list-style-type: none"> ○ release specifications for industry input prior to the final tender being released ○ run an information session/workshop. <p>Publish these opportunities publicly (i.e. on eTendering) to give all prospective tenderers an opportunity to participate.</p>
<p>Misrepresentation of facts by potential IoT service providers resulting in claims of unethical or unfair dealing, or breach of contract</p>	<ul style="list-style-type: none"> • Independently verify service provider qualifications. • Conduct due diligence checks such as past convictions, corruption findings, bankruptcy or insolvency checks. • Seek referee reports and independently verify their accuracy. • Confirm adequate performance if the IoT service providers have previously supplied to government.

Procurement risk	How to avoid it
<p>Selection of inappropriate procurement strategy leading to an inadequate or inappropriate result and/or not achieving value for money</p>	<ul style="list-style-type: none"> • Consider your business needs, key risks, and opportunities. Be clear on your desired procurement outcomes. This must be reflected in your procurement strategy (check out the NSW Procurement Approach for a Procurement Strategy template). • Engage early with your procurement team and other experts. • Research the market so the procurement strategy is effective within current market dynamics. • You can also consider: <ul style="list-style-type: none"> ○ A collaborative or staged market approach (e.g. competitive dialogue, Expression of Interest or request for proposals) then seek tenders from the best respondents. ○ Negotiating with best performing IoT service providers to improve value for money and/or responses (your tender documents should allow you to do this). ○ Running a limited tender if it is clear that a limited number of IoT service providers can meet your requirements (following an open tender). Note there are restrictions on this if your procurement is covered by the enforceable procurement provisions (see the PBD-2019-05 Enforceable Procurement Provisions).
<p>Inappropriate evaluation criteria leading to inadequate or inappropriate response, or not achieving the best value</p>	<ul style="list-style-type: none"> • Negotiate with the best performing IoT service providers to improve value for money and/or responses (your tender documents should allow you to do this). • Go to market again – consider using a staged procurement approach if the specifications are not clear and revise the evaluation criteria so that it will adequately assess the solution.
<p>Terms and conditions are unacceptable to IoT service providers leading to higher costs, tenders with numerous</p>	<ul style="list-style-type: none"> • Use standard terms and conditions (where they exist) or develop commercially accepted terms that are tested with the market. Avoid onerous reporting requirements, short delivery timeframes or departure from industry standards. • Do not try to contract out of all risks. The best practice is to allocate risks based on who is best placed to manage them. Do not ask IoT service providers to carry a risk that is outside their control.

Procurement risk	How to avoid it
qualifications/exemptions, or no/limited number of tender responses	
Actual or perceived breach of confidentiality where a tender respondent's intellectual property/commercial information is not protected, resulting in IoT service provider complaints, mistrust or political intervention	<ul style="list-style-type: none"> • Establish formal security procedures to ensure tenders are handled securely: <ul style="list-style-type: none"> ○ Use eTendering to manage the receipt of tenders and secure systems to store information ○ Restrict access to tenders to the evaluation committee and/or make staff with access to tenders sign a code of conduct and declaration of conflicts of interest ○ Check conflict of interests arising during evaluation at the start of each meeting ○ Keep thorough records, record any conflicts and mitigation actions. • Perform regular security audits and reviews, advise IoT service providers of security measures, and train staff.
Organisation does not own IoT data collected and the IoT service provider limits or prevents the organisation from accessing the data	<ul style="list-style-type: none"> • The procurement specifications and the contract need to explicitly state who owns the raw data. It is recommended that your organisation owns the raw data to give you flexibility to use the raw data for other purposes (e.g. data analysis and combining with different data sets).
Selection of inappropriate goods/services means the IoT service provider's solution does not meet the desired outcome	<ul style="list-style-type: none"> • Involve end-users in the evaluation • Make sure the evaluation panel has or can access the relevant technical expertise. Refer to the UN Procurement Practitioner's Handbook for more information.

6.1.8 Disposal of assets

The final stage in the procurement process is the disposal of assets that have reached the end of life. Disposal is considered 'procurement' under the [Public Works and Procurement Act 1912 \(NSW\)](#) and is governed by the [NSW Government Procurement Policy Framework](#) and [NSW Procurement Board Directions](#).

Your project should address end of life planning for disposal of 'things' and associated assets. For example, on-selling if items can still be used, repurposing, recycling useful or valuable materials, appropriate disposal of hazardous items.

Disposal can be factored into the procurement strategy. Manufacturers or suppliers may have established recycling or repurposing programs already in place. If so, this can be written into the tender and resulting contracts.

6.2 Data considerations for contracting

It is critical to clearly address data requirements in contracts with IoT service providers. Contracts need to address the matters outlined in this chapter.

6.2.1 Data handling

IoT solutions often need multiple IoT service providers to provide hardware, software, and connectivity. You need to require service providers to perform due diligence and identify all parties involved in developing and delivering these products and services.

You want transparency from your service providers about their data handling and storage practices so that you have full visibility of all parties who have access to the data generated by your devices.

6.2.2 Data ownership and rights

a) Data ownership and control

Identify who owns the data under the contract and ensure your contract enables you to have all reasonable control over your data. Define your data governance requirements in contractual approaches and stipulate your requirements for what data is being collected, where it is stored and who can access it, at what granularity and for what purpose.

If the IoT service provider owns the data, identify whether they are entitled to sell the data about your performance to a third party, and understand any contractual rights to see, use and monetise this data. If this use is unacceptable, look for other service providers who have data policies that give you rights to your data for ownership, use and reuse purposes.

Case Study – Intellectual property and data access

One local council tried to gain access to parking data collected as part of its 'smart parking' software trial. Unfortunately, under the terms of the contract, the data was not exportable from the app provided by the software supplier. This limited data reuse potential.

Ensuring you can access and use any data collected by sensors is an integral part of the planning and contracting process for IoT-enabled projects.

Organisations enabling IoT deployments often have direct legal responsibilities to persons affected by the use of those IoT deployments, even if the use of the IoT deployment is by other entities (such as third-party service providers). You need to clearly stipulate in the contract the rights and responsibilities of each entity within a data ecosystem. 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.

IoT service providers are subject to NSW data laws, such as the [State Records Act 1998 \(NSW\)](#), [Privacy and Personal Information Protection Act 1998 \(NSW\)](#) and [Government Information \(Public Access\) Act 2009 \(NSW\)](#).



Tip: Software development is the major growth area in IoT as commercial organisations look to leverage the power of data generated through IoT initiatives. If your organisation is likely to leverage this type of software, consider data 'ownership' and rights of data use and disclosure in your contract.

b) Exclusive rights to use of data

All contracts and design processes should make clear that exclusive rights to use of IoT data generated or facilitated 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.

c) New datasets

A new dataset may be generated as part of your IoT 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.

You may also need to consider whether monetisation and intellectual property of data and trained machine learning models also need to be addressed in your contract arrangements.

d) Data retention and destruction obligations

All government data held by an IoT service or 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 an IoT service provider is discontinued.

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.

6.2.3 Data quality requirements

a) 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, use your contract to define data governance requirements and required mitigations that minimise the likelihood of these risks. This can include:

- service level agreements with IoT service providers for fault identification, remediation and re-calibration of devices at regular intervals
- acceptable standards for data quality
- uptime and availability requirements.

b) Liability arising from data quality

You 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. Depending on the strength and resilience of your IoT network, 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 IoT 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 IoT 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, seek legal advice on appropriate wording and include a disclaimer in any licence agreements. Disclaimers will not eliminate complete risk, but a combined metadata statement, licensing agreement and disclaimer is a suitable method for risk mitigation.

6.2.4 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 you have specified.

Depending on the purpose of your IoT-enabled project and the nature of the data you are collecting and using, you may want to address monitoring and mitigation responsibilities for software and hardware vulnerabilities in your contract. If these vulnerabilities lead to data insecurity or privacy impacts, you should define liabilities and responsibilities in the contract.

Be aware of device default settings that may be in place for scenarios like when a device loses connectivity. Default settings may route data back to the device manufacturer if a device loses connectivity. This can be a security and privacy risk and could result in data loss. Require full disclosure of any such default settings in contract and procurement processes and evaluate any reported default arrangements against corporate risk frameworks.

6.2.5 Application Programming Interfaces (APIs)

An Application Programming Interface (API) developed by a third party or provided as part of a commercial product should support the release of open data and maintain the safeguards for personal, health or other sensitive information. Take care to understand and determine what functionality is available via the API as typically this is controlled by the service provider. More information on APIs and data is available in [3.8 Technology for IoT](#).

Commercial agreements relating to the development and use of APIs should be open and transparent. The NSW Government API Standard can help agencies to develop, procure and implement API solutions and tools, see the [Digital.NSW website](#) for information.

6.2.6 Cloud storage

NSW Government has evaluated and endorsed a panel of cloud service providers that are available to agencies to contract via <https://suppliers.buy.nsw.gov.au/browse/suppliers>.

For contract arrangements with cloud providers, you need to ensure that:

- the data needed to support business operations is created and kept for as long as they need it
- ownership of government data remains with the State
- if IoT data legally needs to be kept for longer than the service agreement period with a specific service provider, the contract and operating arrangements enable this data to be returned to State ownership in accessible and useable forms once service arrangements conclude
- if specific IoT data is no longer needed for business operations and can legally be destroyed, this destruction is identified and authorised by the organisation and is accountably performed by the service provider on the organisation's behalf.

Avoid cloud storage lock-in relationships that can come with specific device-hosted cloud arrangements. You want the ability to store and process data in ways that best work with your technology stack.

6.2.7 Establishing clear responsibilities

Be aware that the day-to-day operation of data custodial responsibilities may be delegated or contracted to other parties under your IoT service arrangements, but the overall responsibility for data rests with your organisation.

Under the [State Records Act 1998 \(NSW\)](#) government organisations are responsible for the creation, management, protection and maintenance of their datasets, even when these management responsibilities have been delegated to another organisation. To mitigate potential breaches of the *State Records Act 1998*, custodianship agreements must be in place that outline data creation, management, retention and destruction requirements. Responsibilities under the [Government Information \(Public Access\) Act 2009 \(NSW\)](#) and [Privacy and Personal Information Protection Act 1988 \(NSW\)](#) must also be clear.

6.3 Key contract terms for IoT solutions

This table contains key contract terms you should consider when developing a contract for an IoT solution. It is not an exhaustive list of areas that need to be included in a contract.

Contract term	What needs to be covered in the contract?
Data	See Chapter 5.2 Data considerations for contracting .
Privacy	<ul style="list-style-type: none"> Any relevant privacy provisions. For example, the IoT service provider may be required to have and maintain a privacy policy, data security policy and/or audit requirements to ensure the service provider's compliance in relation to the principal's data held by the service provider.
Intellectual property	<ul style="list-style-type: none"> Specify who owns the intellectual property. The NSW Government default position is that the service provider owns the intellectual property and must grant a perpetual, transferable, royalty-free licence for the NSW Government agency to use it.
Transfer/right of use by other agencies	<ul style="list-style-type: none"> The contract should consider the need to transfer contracts, products or licences to other organisations in future (for example, due to Machinery of Government changes).
Multi-agency access contracts "Piggybacking" clauses	<ul style="list-style-type: none"> Piggybacking is where one organisation has established an arrangement and has made the arrangement available to other organisations. Piggybacking requires organisation to accept the terms and conditions of the existing contract. You need to consider if it is appropriate to permit other organisations to use the contract. Guidelines on the inclusion of piggyback clauses and sample clauses to be incorporated into market documents can be found at https://buy.nsw.gov.au. At a minimum ensure the contract does not include a confidentiality requirement that prevents the contract being provided to other organisations.
Supply chain integrity	<ul style="list-style-type: none"> An IoT service provider must maintain the integrity and security of its supply chain. This includes contractual undertakings for the IoT service provider to provide the client with information about its local and global supply chain as it relates to, or impacts on, the hardware and software provided as part of an IoT network. For more information on supply chain risk, see the Cyber security chapter.
IoT service provider conduct	<ul style="list-style-type: none"> IoT service providers must meet minimum standards of conduct in ethical behaviour. If they breach the expected level of behaviour (corruption, fraud, breach of govt policy, etc.), you need to reserve the right to take action, up to and including termination of the contract.

7. Set up

Best practice considerations at this stage in a project

- Is a comprehensive change management plan in place for pre-and post-go live periods, and have the affected business unit(s) been involved in this plan?
- What communications are planned for release or for live transition?
- Is training and support adequate? Is ongoing support provided to those affected by the change?
- Are there any legacy systems, and are the plans to transfer data, integrate with them and exit them adequate?
- Have you documented the key decision points and information needed for the ongoing operation of the solution?
- If applicable, is the operations or delivery team ready to take over and manage the operations and have you transferred asset information to them?
- Has adequate time been allowed in schedules to fix faults and are there arrangements for proactive monitoring and management of any slippage?
- Are there business contingency and continuity arrangements and plans that aim to minimise the impact on the business in the event of major problems during implementation and rollout?

7.1 Change management

This chapter provides guidance on internal change management, to assist with managing change brought about by new IoT solutions in an organisation.

7.1.1 What is change management?

Introducing new and innovative tools and practices such as IoT can result in periods of unrest for affected people including staff, customers and other stakeholders. While change can be exciting for some, for others change means loss, disruption or threat. Effectively managing the people and process side of an IoT-enabled project is essential for a successful implementation.

Change management is the process of taking a planned and structured approach to help align an organisation with change. It is about supporting and understanding people who are undergoing change and handling that change with minimal disruption.

In an IoT context, change management means working with the stakeholders affected by the IoT-enabled project and the accompanying new processes, to help them:

- understand what the change means for them
- navigate the transition
- understand the value of the IoT-enabled project
- to overcome challenges together.

7.1.2 Why is change management necessary?

Effective change management allows organisations to deliver new initiatives, embrace evolving technology and adapt to new environments more easily.

Change management is necessary for IoT-enabled projects because people are integral to the successful adoption and integration of IoT. You may have all the right processes in place but if the people involved in the IoT-enabled project do not understand the change and why it is happening, your project may be at risk.

It is important to remember that systems and processes impacted by IoT have a human element, and the people impacted will have different levels of technology awareness and enthusiasm for change.

7.1.3 Managing change resulting from IoT-enabled projects

There is no one size fits all approach to change management. Change management requirements and best practices differ by organisation and subject area. There is currently no whole of NSW Government change management policy or guidance.

When managing change for your IoT-enabled project you may consider:

- *Vision and objective:* Do you have clear definitions of your goal and why the change is happening? Are the people affected aware of these and do they understand them?

- *Trust*: Do the people affected know they can trust you to do this respectfully and with minimal disruption?
- *Consultation*: Will people be consulted about the changes? How much influence will they have?
- *Journey*: Is every stakeholder on the change journey with you? Do they know what you are trying to achieve and why? Do they understand it?
- *Communications*: Are all stakeholders aware of the important pieces of information? Is there a way you can be more open and transparent?
- *Executive support*: Does the change and change management plan have the support of senior managers and executives in your team?
- *Training*: Has there been enough training provided? If not, how can you get everyone on the same page?

7.1.4 Managing ICT infrastructure change

a) ICT infrastructure change management

For the purpose of this policy, managing infrastructure change refers to changing ICT infrastructure systems (not managing the impact of change on people). An example is replacing legacy systems so that IoT solutions can integrate with your organisation's ICT systems.

There is no one size fits all approach to managing ICT infrastructure change. Speak to your agency's IT/Operational Technology team for further information and assistance about the matters in this section.

b) What are legacy systems?

Legacy systems refer to ICT infrastructure systems that are outdated but continue to be used over updated versions of the system (or a new system altogether). Legacy systems continue to be used for various reasons (e.g. they may have been custom-built or the cost of changing and re-training staff is too high).

Some legacy systems may not be capable of integrating with new IoT systems and will need to be replaced for an IoT solution to be adopted.

c) How to integrate new technology with old technology

There is no one size fits all method of integration/migration of systems or data to work with your IoT solution. As each organisation's ICT infrastructure is different, it is important to assess your infrastructure to determine the best solution for your scenario.

When assessing your current infrastructure, consider:

- What is the current state of your ICT?
- How old is the technology?
- Is the technology still compatible with your current business needs?

- If your current ICT system is one that is working and meeting business needs, where are the connections between the current infrastructure and the IoT solution you want to introduce?
- If you decide to replace your current ICT system, what kind of solution meets your business needs, including the needs of the IoT solution you want to introduce?

Depending on your ICT infrastructure and the responses to the questions above, you may require expertise in migration to new systems and integration of IoT systems with legacy systems. It is important to undertake this transition properly as rushing can result in a loss of data and/or lead to larger costs down the track.

There are many approaches to introducing IoT systems. Three options are:

- remove and replace the legacy system with an IoT-enabled system
- integrate the legacy system with a new IoT-enabled system
- develop a custom solution that mixes both.

Speak to your organisation's ICT team for further information on legacy systems.

7.1.5 Additional resources

See the [Queensland Government's Change Management Best Practices Guide \(2014\)](#) for further information on what change management is.

The Government of South Australia has developed a [Change Management Toolkit](#) that provides guidance and resources to assist organisations to manage people through a process of change.

Also, speak with your organisation's change management team and check your intranet/website for organisation-specific resources.

7.2 Spatial data requirements

7.2.1 What is spatial data?

Spatial data refers to the location, shape, and size of an object tied to the Earth's surface. Datums provide the conventions by which coordinates in latitude and longitude (or other coordinate types) and height describe the real-world location of features on the Earth.

A road map is a common example of spatial data. The location of cities, roads, and boundaries that exist on the surface of the Earth are projected onto the map, preserving the relative positions and distances. The data that indicates the Earth's location of these cities, roads, and boundaries (i.e. longitude and latitude) is the spatial data.

7.2.2 Introduction to the NSW Digital Twin

The NSW Government is developing a Spatial Digital Twin, or digital model, of NSW that is supported by an ecosystem of data, platforms, infrastructure and governance arrangements. It will be relevant for urban and regional planning and development,

emergency management, natural resource management and environmental management. The NSW Spatial Digital Twin will provide the platform upon which government, developers and residents are able to visualise, plan, develop and assess infrastructure (such as transport links), new community facilities, public spaces, and homes.

Currently in NSW authoritative 2D foundation spatial data – that is, a map of the State – is used across government, industry and the community to inform decision making and planning. However, 2D foundation spatial data does not leverage the full capabilities of emerging systems, platforms, digital modelling, and monitoring of our natural and built environments. Increasingly infrastructure will be planned, delivered and operated using digital models.

The development of an effective digital model that contains four-dimensional (4D) data sources must include a foundational layer of authoritative 4D spatial data (4D means 3D visualisation with the ability to move forwards and backwards in time). Once a foundation layer is available, specific information can then be overlaid to inform planning for future infrastructure and maintenance of current infrastructure, creating a digital twin that mimics real-world behaviour.

The benefits derived from a digital twin include:

- reducing the cost of capital projects and operating costs of infrastructure
- supporting the construction sector to adopt digital technology
- exploring skills and services in digital technology
- creating real-time learning opportunities by providing access to digital models and improving whole of life integration of infrastructure and place.

7.2.3 Recording IoT device position to meet spatial data requirements

a) Importance of recording IoT device position correctly

Mobile and stationary IoT devices frequently communicate their position, time and status, and may pass this information onto third party systems. An example of this is Cooperative Intelligent Transport Systems (connected vehicles) which uses IoT to enable real-time wireless communication between vehicles, roadside infrastructure, mobile devices, and back-office systems to improve the transport network.

To communicate effectively, IoT devices must be clear on the:

- datum in which they express their position
- date and time that the dataset measured
- quality of the data measured.

An intelligent Geographic Information System (GIS) should consume data in any nominated datum and translate between datums using established standards.

b) Requirements for IoT device spatial data

Data collected by IoT devices can be absorbed into the NSW Digital Twin. To enable this, IoT devices **must**:

- Record device location, including datum:
 - Restricted to datums (or Coordinate Reference Systems (CRSs)) defined by existing European Petroleum Survey Group (EPSG) codes, which includes all internationally known and accepted datums/projections (as well as the official transformations between them). GDA 2020 is recommended.
 - Refer to Standard Data Format Standard:
 - Refer to ISO19111:2019 Geographic information - Spatial Referencing By Coordinates
 - E.g. XML and JSON formats:
 - Geojson, with inclusion of a defined CRS
 - Geography Markup Language (GML), see ISO 19136:2007
- Include a time/date stamp for all observations recorded at the device (time zone to be included e.g. AEST, UTC etc.)

IoT devices **should** also record:

- The time-stamp of the coordinates in the given datum or CRS. Please note ISO 19111:2019 now supports spatial coordinate reference systems in which coordinate values of points on or near the surface of the Earth change with time due to tectonic plate motion or other crustal deformation, and
- Uncertainty value (expression of how well coordinates are known) for each dataset if possible. While this feature-level metadata is desirable, it may not be well catered for by existing standards. At a minimum, location accuracy (known or estimated) should be included in the metadata for the dataset or device.

For **automation** of sensor to Digital Twin data exchange, a standard data format for communicating location is required:

Co-ordinates + Datum (i.e. GDA) + Standard (geojson, GML, etc.) + time and date (include time zone)

7.2.4 GDA2020 and the Australian Terrestrial Reference Frame

In October 2017 GDA2020 superseded GDA94 as the new National Datum of Australia. Since then NSW Government has been working to make data and services available in GDA2020 to support high-precision positioning applications like IoT.

It is expected that from 2023 the continued movement of the Australian tectonic plate (approximately 7cm per year) will necessitate a transition to time-dependent coordination.

In Australia, the Australian Terrestrial Reference Frame (ATRF), along with GDA2020, will cater to this need.

More information on the adoption of GDA2020 and ATRF is available from the [Intergovernmental Committee on Surveying and Mapping](#) and on the [NSW Spatial Services website](#).

7.2.5 Positioning standards

Communication of position and datum information is accomplished by various standards including [PROJ](#), [EPSG](#), [WKT](#). A discussion of some of the technical differences can be found at the website of the [Earth Lab at the University of Colorado](#).

Other standards relating to spatial data are listed in the following table.

Other standards relevant to spatial data

Spatial-related standards	Description
NSW GDA2020 and AGRS Implementation Policy	A geocentric (Earth-centred) coordinate reference system that is Australia's official national datum within the Australian Geospatial Reference System.
AS/NZS ISO 19111:2019 Geographic Information; Referencing by Coordinates	This standard is applicable to producers and users of geographic information. Describes the conceptual schema for the description of referencing by coordinates, and the minimum data required to define coordinate reference systems
ISO 19127 Geographic information	Developed as a Geodetic Registry to supersede/coordinate ISO 19111 to support time-dependent coordinates. See also associated ISO standards from the ISO/TC211 Working Group.
AS/NZS ISO 19162:2018 Geographic information	Provides a well-known text representation of coordinate reference systems, defines the structure and content of a text string implementation of the abstract model for coordinate reference systems.
AS/NZS ISO 19115.1:2015 Geographic Information	Provides the technical definition of the standard and is intended to provide tech-savvy implementers with detailed information for software development and other purposes.
AS/NZS ISO/TS 19139 series Geographic Information XML schema implementation	Defines XML based encoding rules for conceptual schemas specifying types that describe geographic resources.
NSW Standard for Spatially Enabling Information (2018)	Established standards for spatially enabling NSW Government data and information.

7.3 IoT deployment and configuration

7.3.1 Device deployment and configuration

The way that IoT is deployed and configured can have a significant impact on data quality and security. IoT devices need to be configured with attributes such as name, location, and application-specific settings (i.e. the unique ID of the asset the device relates to).

It is also important to recognise that data from your project may be used in a future project. Consideration should be given to a wider set of information being captured such as:

- records for who installed the sensors
- how access for maintenance is managed
- who is responsible for changing batteries, calibration needs, and other responsibilities?
- any commercial constraints or agreements
- any other factors that might make the usefulness of sensor data more valuable on future projects.

IoT devices also need to be managed as configuration items in your organisation and documented for asset management and incident management purposes. This helps them to be trusted components in your organisational architecture and ensures that devices and the data they transmit can be part of organisational data flow.

Appropriate deployment and configuration will establish device monitoring benchmarks; this allows you to proactively identify and remediate real or potential security issues. Testing during the deployment phase ensures that data is being generated and transmitted as expected.

Configuration and adaption should be an ongoing process. You need to ensure business users of IoT data can communicate with device owners and software providers to tailor data collection rates or to drive quality and calibration checks throughout the lifespan of your project.



Tip: An IoT device may use many off-the-shelf software and hardware components. Only a small proportion of these components may be manufactured and maintained by the IoT service provider. Maintaining a Software Bill of Materials for each device may be a good practice to ensure documentation and traceability for all components.

7.3.2 Communicating about deployment

Consider what communication or education your stakeholders may require support about any IoT deployment. This can be supported by a stakeholder engagement strategy. See [Chapter 3.2 Stakeholder engagement](#) and [Chapter 6.1 Change management](#) for further advice.

8. Use and Maintain

Best practice considerations at this stage in a project

- Are you using and analysing the data generated from IoT? Are you using your data to realise new business models or ways of working?
- Is your data in real time or near real time?
- Are you sharing data in line with data sharing and privacy laws?
- Do you have a schedule and are you prepared to conduct cyber security penetration testing?
- Are there ongoing communications keeping key stakeholders effectively up to date with progress and plans?
- How are you collecting data? How will you store and maintain your data?
- Do you have a device or project maintenance schedule in place and are you sticking to it?
- Are you managing your assets in line with [NSW Treasury Asset Management Policies](#)?

8.1 Data analysis and use

8.1.1 The data analytics process

IoT allows for near real-time operational insights (unlike traditional business intelligence based on batch runs that output reports for later consumption). These insights can be provided in terms of alerts or post-processing insights to allow for streamlining processes. The data requirements to source this data and then bring it in for custom analytics are the foundation of data analytics platforms.

Data analytics has an ever-increasing range of applications, including predictive maintenance, remote monitoring, inventory tracking, performance management of devices or networks, capacity utilisation and planning, demand forecasting and customer service improvement.

Examples of types of data analytics used for IoT data

Type of data analysis	Description
Streaming	Also referred to as event stream processing. Used to analyse huge in-motion data sets. Real-time data streams are analysed in this process to detect urgent situations and immediate actions. This type of data analytics is used for IoT applications, including those based on financial transactions, air fleet tracking and traffic analysis. This type of task can often be labelled anomaly detection.
Spatial	Used to analyse geographic patterns to determine the spatial relationship between physical objects. This type of data analytics is used for location-based IoT applications, such as smart parking applications.
Time-series	Based upon time-based data which is analysed to reveal associated trends and patterns. This type of data analytics can be used for IoT applications such as weather forecasting, electricity consumption, and health monitoring systems.
Prescriptive	This form of data analytics is applied to understand the best actions that can be taken in a particular situation.

a) Steps for data analytics

To perform data analytics, processes need to be adopted and generally encompass:

- [data requirements specification](#)
- [data collection](#)
- data cleansing
- any required [privacy preserving measures](#), such as anonymisation and deidentification
- data modelling

- data visualisation and communication.

The data analytics processes for data cleansing, data modelling, and data visualisation and communication are described below.

1) Data cleansing

One of the first steps of data analytics is to cleanse the data. With the definition and metadata of IoT devices, the data cleansing process can be greatly reduced as spelling mistakes and nonsense data will hopefully be caught in [data validation processes](#). The definitions of data schemas at the device level can also help to reduce the quantity of data cleansing required.

Data cleansing is vital for accurate data (incorrect data can generate misleading results). Analysing your data and using techniques to automate these error checking methods can help to speed up this process. A data analyst still needs to be involved to investigate any issues.

2) 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.

If using a public model, ensure it is secure and does not include Trojans or other malware. If making your model public, ensure that no information is inadvertently leaked in the release and that there is no potential for inference attacks.

The optimisation process will begin once the initial model is developed. This process is often iterative as the best answer will not always be your first one. By automating the data process at various stages, you can leverage the continuous improvements found from the data insights.

For IoT sensors, the faster you can learn from your data, the quicker you can course-correct if required for streaming problems. When dealing with prescriptive or time-series data sets, the more data you feed into a machine learning algorithm the better able it is to improve and deliver better outcomes. Therefore, optimisation and repeatability are vital for quick results. However, more data does not always result in better outputs. Accessing the right data is a bigger priority.

3) 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. Note that licences are required for most visualisation tools.

There are a range of different data visualisation offerings ranging from smart-dashboards, 3D Visualisations and even augmented reality capabilities. Each offer differing capabilities and vary significantly in cost, so more time must be spent evaluating the best and most

effective way data will be consumed by the intended users of data. The interfaces need to be intuitive and informative without being complex

There are various dashboarding tools that can be used to present IoT data visually to stakeholders. For IoT devices that are often near real-time, these can be dashboards where a user is monitoring the data for any outliers and alerts triggered for data above certain thresholds or outliers detected. These are common in industrial production uses of IoT.

The type of dashboard and alert system built for a streaming analytics user will be different to that built for a user who is more interested in time-series and trend analysis and make overall business improvement outcomes. These requirements can still ingest real-time data, but the dashboard display will be focused on data models and insights from machine learning algorithms around their outcomes and areas of identified opportunities.

Another common way to visualise data is via spatial systems, including the emergence of enhanced 3D spatial platforms and digital twins. It is important that these systems can seamlessly show real-time ingested data with existing spatial data (including mixing 2D and 3D data) and support a range of traditional 2D and emerging 3D spatial analytics operations.

b) Next steps after the data analytics process

Analytics can help you solve a question and machine learning is often used to help understand what data attributes may be affecting a result. By combining various datasets and learning from previous events, you can leverage knowledge and make insights and outcomes smarter through analytics.

Once the business outcomes are delivered, leveraging the data to identify new ways of operating and new service innovations can be explored. The new data you are generating can be used to develop insights and innovations across your organisation or potentially to offer value more broadly.

Case study – An example of the application of modelling and analytics

IoT water sensors may be used to determine flood levels. While it is useful to read an individual water meter, the real value of the analysis is in the ability to read the whole network at once. This allows you to build and see a holistic model of the water situation, identify patterns and develop alerts to determine when a system is at risk of flooding.

The next step is to start using the IoT data and build analytics to learn and make data models smarter, which can be done by implementing machine learning and artificial intelligence. This is a step change from visualising the data, to building algorithms, to start learning from the data and linking this to outcomes.

Predictive analytics is valuable as it allows you to leverage the alert systems, and identified anomalies from the data and historical data from the last flood to learn how to improve the predictive flood analysis model.

Case Study – NSW Health’s Proactive Sepsis Management project

Every year more than 60,000 Australians are diagnosed with sepsis. 15,700 of those patients are admitted to Intensive Care Unit at an estimated cost of \$39,300 per episode, equating to \$617m annually. The annual death toll from sepsis is more than 5,000, which is greater than the annual national road toll and sepsis causes more deaths than breast, prostate or colo-rectal cancer.

The Proactive Sepsis Management project is first of its kind to provide real-time integration of medical devices using IoT in the world. It is a partnership between NSW Health Pathology (NSWHP), eHealth NSW and Western Sydney Local Health District (WSLHD) to significantly reduce sepsis deaths and negative patient outcomes. The project will:

- develop an IoT Diagnostics Pipeline for the transmission of data from medical devices not directly connected to existing electronic Medical Records
- leverage artificial intelligence and real-time analytics to produce a real-time dynamic risk stratified list of at-risk sepsis patients in the emergency department waiting room for action by clinicians

By providing a real-time clinical support tool, the project aims to see a reduction in time to administration of antibiotics, resulting in a significant reduction in patient deaths and improved preventative measures. Once a patient has antibiotics administered, their probability of death reduces by 7.6% per hour.

The *IoT Diagnostics Pipeline* will consume, digitise and automate the collection, transmission and storage of a patient’s vital signs data in real-time. With the use of mobile connectivity technologies (LTE, Wi-Fi and Bluetooth), the IoT Diagnostic Pipeline can connect medical devices directly to IoT gateways without requiring fixed hospital IT infrastructure.

The benefits of the project across stakeholder groups include:

- for clinical staff, automating patient observations data reduces workload while the analytics will deliver a tool providing real-time risk stratification of patients in the Emergency Department to support their clinical decision-making
- for clinical staff, by removing the need for manual transcription of patient vital signs from device into FirstNet. Current practice does not include having another staff member co-check result entry, leaving room for risks associated with transcription errors
- patient outcomes will improve with faster clinical decision-making and treatment resulting from real-time clinical results, even in settings where it was not previously possible

- for the health system, the tools will provide opportunities to manage patients in and out of hospitals more efficiently. By proactively treating patients, inpatient visit times will be reduced and hospital resources better utilised

The Proactive Sepsis Management Project has made the following achievements since commencing in April 2019:

- IoT Device Provisioning time reduced from two days to 40 minutes
- Result transmission down from hours to minutes to sub 20 seconds
- Multiple pathology PoCT devices implemented
- First non-pathology device (vital signs) integrated
- Robust and extensive testing using IoT Diagnostics Pipeline, with automated testing solutions
- IoT Pilot production testing and evaluation in seven metropolitan and regional locations
- IoT remote monitoring and management solution
- IoT Gateway manufacturer evaluations
- Development of front-end decision support tool, for risk stratification off all patients within ED

8.1.2 Using data for your business outcomes

You can use data to continuously track and measure the business outcomes you defined at the start of your project. Without clear definitions of what constitutes success at every stage, progress can lag, data collection and use can become costly and untargeted, and the value of IoT initiatives can be diminished.

You can also leverage the data to identify new ways of operating and explore service innovations and improvements once your business outcomes are delivered. Consider how your data can be leveraged more effectively across your business or be made available

If your organisation is planning to (or is) commissioning new infrastructure assets, a data and IoT strategy for each new government asset should be created.

The [Smart Infrastructure Policy](#) sets out the minimum requirements for smart technology (including IoT) to be embedded in all new and upgraded infrastructure from 2020.

The [Infrastructure Data Management Framework](#) provides guidance on implementation and management specific to government infrastructure. This will assist with ensuring the benefits from IoT, and the IoT foundations you have developed can be leveraged.

8.2 Data sharing

8.2.1 Why and how to share data

A fundamental requirement and key enabler of IoT systems is the ability to access, share and use data that has been collected. You can ensure that you own the IoT-generated data and that you can share it by addressing [data ownership in your contract arrangements](#).

There is value in sharing your data with another organisation or third party. In fact, your project may specifically require data sharing. For example, the creation of smart cities relies on sharing data collected by local and state governments as well as private organisations. Data sharing can lead to benefits such as:

- enhanced competition and innovation
- greater system-wide resilience and capacity
- opportunities to share insights and increase the scope and value of collected data.

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

To share data in more controlled ways with trusted third parties, you can:

- make data available to third parties for them to process and use, potentially via an API
- control data access but allow trusted third parties to submit analysis algorithms to the data, to derive insights from it.

Sharing data or the insights generated from your IoT-enabled project with trusted third parties will require you to specify the necessary data standards and data quality to enable [interoperability](#).

Data sharing can be facilitated by use of common platforms, including open data platforms such as data.nsw.gov.au for the sharing of publicly available open data, or shared data platforms or federated networks for sharing of more sensitive data. A secure federated data access model enables permission-based access to available data for trusted parties.

Additional guidance on the benefits and purposes of data sharing is available at Data.NSW, including the following at: <https://data.nsw.gov.au/developing-business-case-data-sharing>

Better access to data leads to better customer service and a more efficient government

- Data is a key element of the digital transformation of NSW government

- NSW government is moving to responsive models for decision making, which are aided by access to data
- Access to more data allows agencies to more rapidly measure their approaches, and adapt based on evidence
- Access to more data can lead to better informed investments and more comprehensive planning
- Data sharing can enable better collaboration across all levels of government, to develop coordinated and evidence-based approaches.

8.2.2 Responding to requests for data sharing

Data sharing may be initiated by the owner or producer of data but is generally initiated by a request to a data owner.

It is best practice to follow the steps in the following table when you are looking to share IoT data. This information is a guide only. You should seek detailed advice from your privacy contact officers, legal officers, and the [Information and Privacy Commission NSW](#) to confirm your data-sharing arrangement is lawful, ethical and safe.

Steps for data sharing

Step	Description
<p>1) Can the data be shared legally and under what conditions?</p>	<ul style="list-style-type: none"> • Certain laws and regulations prevent or limit the scope of sharing some forms of data. You must consider your legal and compliance obligations with respect to whether you can share the data and under what conditions. • <i>Does the data requested contain personal information?</i> Under the Privacy and Personal Information Protection Act (1998) (NSW), personal information may only be used or shared for the purpose for which it was collected, or for a secondary purpose if an exception applies. You must determine whether the sharing of personal information with a third party is compatible with the original purpose it was collected for and the privacy policy and/or notice given to the individual. If it is not compatible, the data that contains personal information must be de-identified. If the data is successfully de-identified, the modified data will no longer trigger privacy legislation. Step 3 explains how to de-identify data. • <i>Does the requested data contain other sensitive information?</i> Legal restrictions prohibit the sharing of some forms of sensitive information, such as data protected by intellectual property rights, data considered confidential (including trade secrets), financial data, etc. This data cannot be shared in its raw format, except in exceptional circumstances. A decision not to share data should only be made after consultation with your organisation’s legal officers and after all attempts have been made to protect the sensitivity of the data. • <i>Exceptions?</i> In some instances, the sharing of sensitive and personal information in its raw form is legally permitted, such as: <ul style="list-style-type: none"> ○ where the data subjects have given consent ○ where it is necessary for the performance of government duty that is in the public interest ○ where it is necessary for the purposes of the legitimate interests pursued by the organisation disclosing the data, or the party receiving it, as balanced against the rights and interests of the data subjects.

Step	Description
	<ul style="list-style-type: none"> • <i>Will the requested data be linked with one or more datasets?</i> Just because data does not contain sensitive information does not mean that it will not become sensitive once it is shared. Non-sensitive data may become sensitive when the data is linked with one or more datasets that include information about the same person or some subject. For example, location data, identification numbers or online identifiers, such as IP addresses, cookies, and RFID tags, can provide ways to make data personally identifiable. Talk to the data requestor about how they intend to use the data. • <i>No legal or compliance issues identified?</i> If there are no legal or compliance issues, you should consider making this data publicly available in accordance with the NSW Government Open Data Policy.
2) Is the use of the data appropriate?	<ul style="list-style-type: none"> • Use of data that is not appropriate may lead to poor or detrimental decisions. To determine whether the data is appropriate, consider: <ul style="list-style-type: none"> ○ whether the data will be used to provide a public benefit ○ whether the data requested is fit for purpose. • NSW Government agencies have a legal and ethical requirement that data may only be shared if the data satisfies a public interest purpose test. Before sharing your data, you must check with the data requestor to see if the data will be used to inform: <ul style="list-style-type: none"> ○ government policy ○ research and development with a public benefit ○ program design, implementation, and evaluation ○ delivery of government services. • Where appropriate, consult with relevant stakeholders on how to provide the data and ensure it is used appropriately. This means being transparent and creating opportunities for stakeholders and citizens to provide input on proposed data-sharing agreements.

Step	Description
	<ul style="list-style-type: none"> • You need to determine if the data requested is fit for purpose: <ul style="list-style-type: none"> ○ As a data owner, you have the best understanding of what can and cannot be achieved with the data you hold. Speak to the data requestor about their purpose of the data use and if the data can support it. It is also best practice to attach a Data Quality Statement to the data-sharing agreement. ○ If machine learning was used, document the confidence level in the processed data and share this with the end-user.
<p>3) Is there any privacy and/or security risks that need to be managed?</p>	<ul style="list-style-type: none"> • Data that does not contain sensitivities may not require extensive consideration of privacy and security risks. However, if the data contains personal information or other forms of sensitive information, the data should only be shared once privacy and security risks have been identified and managed. See chapter 3.5 Privacy for advice. • Managing privacy and security risks can be managed with a range of risk-management controls, including: <ul style="list-style-type: none"> ○ Using the ‘Five Safes’ (an internationally recognised risk management model). Control access to the data across the ‘five safe’ dimensions to ensure sensitive data is protected and only used by trusted staff for approved purposes. See Appendix E for a description of the Five Safes. ○ Applying disclosure control techniques to the data (e.g. removing direct identifiers or suppressing individual records) ○ Providing aggregated insights instead of sharing raw data. • It is best practice to apply a mix of risk-management controls when sharing sensitive data. For example, IoT data can be encrypted and then stored on a cloud server which only the data requestor can access. A data-sharing agreement can also be developed to formalise the terms of access. Applying a combination of controls helps to ensure that: <ul style="list-style-type: none"> ○ the data recipient is authorised and equipped to use and interpret the data ○ the data recipient uses the data in an appropriate manner ○ neither the environment the data will be stored in, nor the data output will pose risks. • Safeguarding techniques should only be applied to data if there is a good reason to do so. Too much tinkering with the data may result in safe but poor quality and ultimately useless information. For example, the provider of a predictive maintenance solution may want the serial number of devices, real-time error codes, and maintenance schedule for the

Step	Description
	<p>plant. Any form of aggregation compromises the ability of the solution to function properly, Hence, de-identification and aggregation in this case are not fit for purpose.</p>
<p>4) Formalise the arrangement through a data-sharing agreement</p>	<ul style="list-style-type: none"> • A Data Sharing Agreement (DSA) is a document between the data owner and the data recipient/s that sets out the terms and conditions of the data-sharing arrangements. <ul style="list-style-type: none"> ○ There are many forms of data sharing agreements, some are legally enforceable, and some are not (e.g. a Memorandum of Understanding (MoU)). ○ The NSW Government has an MoU template. It is best practice to make data sharing agreements publicly available to maximise transparency. ○ Formally documenting the details of your sharing arrangement is a useful governance mechanism that provides transparency and clarity for all parties involved. • DSAs typically cover: <ul style="list-style-type: none"> ○ what data should be made available ○ who can access and (re)use the data ○ what can the (re)user do with the data ○ whether or not they have the right to distribute the data ○ technical means of data access and transfer ○ frequency of data access ○ data protection/security/confidentiality obligations ○ Data breach notification requirements ○ Liability questions and audit rights for both parties ○ duration of the agreement ○ termination of the agreement

Step	Description
	<ul style="list-style-type: none"> ○ costs (if applicable) ○ governing law and competent court. ● The DSA should identify who owns the devices, data, and insights derived from the data, and who is responsible for dealing with privacy notifications. In some cases, a dataset can be a combination of several sources so it is vital that ownership is articulated and agreed upon. ● Consider how your DSA can meet the specific needs of the user so that mutual benefits are realised. Consult with the data requestor to determine the most appropriate DSA.
5) Monitor compliance with the data-sharing agreement	<ul style="list-style-type: none"> ● Monitor the agreement to verify compliance with the terms and conditions.

8.3 Asset, device and data management

This chapter provides advice on the management, maintenance, and disposal of IoT assets including devices and data.

8.3.1 Asset management

Asset management is the coordination of activities to realise the value of assets. It involves managing the risks and opportunities of assets to achieve balance across cost, risk, and performance.

a) Relevance for IoT-enabled projects

An IoT solution is not a set and forget project as certain elements will require ongoing management and maintenance:

- physical assets, including sensors and devices
- information assets, including the data collected by the IoT solution
- ICT assets, including software and data management systems
- infrastructure assets
- movable assets.

IoT asset management can provide opportunities to improve services and outputs through the regular assessment of devices, software and data performance so that you can determine areas for improvement.

Ongoing maintenance and management of your devices will allow you to track, monitor, manage, secure and sustain the connected devices. It can also help reduce maintenance and operational costs by minimising significant works and repairs.

b) Asset management plan and asset maintenance plan - why are they important?

A good way to manage assets is via an asset management plan. An asset management plan defines the lifecycle for each component of the asset category (in this case IoT). For instance, the lifecycle of a sensor might be ten years, the lifecycle of a device (transmitter) maybe five years, and the lifecycle of an IoT Platform maybe seven years.

An asset management plan can help you identify how you will manage each asset component over its lifecycle, what the trigger criteria is for replacement (e.g. obsolescence, failure rate) and how to plan for the costs of asset replacement.

Similarly, developing a maintenance plan for your IoT-enabled project can help ensure it does not experience disruption due to preventable repairs and errors. A maintenance plan sets out a plan for replacing, repairing and upgrading assets. It determines the work required to efficiently and effectively address the risks of asset ownership and use as well as their impact on service delivery.

A maintenance plan should ensure that assets continue to support the planned delivery of services, identify any deferred maintenance requirements and establish a funding plan.



Tip: It is rare that a project team wholly owns all components of an IoT solution. Therefore, it is critical to discuss maintenance requirements with the stakeholders who are responsible for the assets not under your control.

c) **How to manage assets and develop a maintenance plan**

The NSW Government has developed [Asset Management Policy TPP 19-07](#) that considers asset lifecycle costs, performance, risk, and economic modelling to support the strategic priorities of the NSW Government.

You may also find it useful to refer to the Australian standard [AS/ISO55000:2014 Asset management – Overview, principles, and terminology](#). This Australian standard is equivalent to ISO 55000:2014. It provides an overview of asset management, its principles and terminology, and the expected benefits of adopting asset management. It can be applied to all types of assets and by all types and sizes of organisations.

d) **Disposal**

Disposal of assets is required when asset reach their end of life. Your project needs to address end of life planning for disposal of ‘things’ and associated assets. For example, on-selling if items can still be used, repurposing, recycling useful or valuable materials, and appropriate disposal of hazardous items. See [Chapter 5.1 Procuring IoT Solutions](#) for information on incorporating disposal of assets into your procurement strategy.

8.3.2 **Device maintenance**

Device maintenance is part of asset management. Traditionally, device and software maintenance at scale has been the domain of telecommunications providers as their customers need to manage a very large number of devices.

However, many IoT-enabled projects by the NSW Government and local governments are likely to be smaller in scale and therefore do not require a telecommunications provider to be responsible for maintenance. This means it is critical to ensure that device maintenance is planned and conducted from deployment for all projects irrespective of their size.

a) **Hardware maintenance**

Hardware in an IoT ecosystem will require maintenance. This includes the devices which may need replacing and new batteries if running on battery power. It is good practice to factor these upgrades into a maintenance plan to avoid any service outages.

Many aspects of the data collected about IoT sensors will be used for maintenance purposes. Typically, almost a hundred points of information *about* a device are collected separately from the sensor data itself. This includes information such as who installed the device, who has access to repair it, when the battery life began, what keys are needed to access the device and the location of the device.

b) Software maintenance

IoT solutions include software that will require bug fixes and software updates. This is generally conducted on an as-needed basis when updates are available. Software updates can contain changes to improve the performance, stability, and security of your IoT systems. Installing updates will ensure that devices continue to run safely and efficiently.

Over-the-air updates, where a device can be updated through the network, allow an IoT platform to track and monitor a device, maintain its software, manage firmware, fix bugs, add features and customise devices even once the device has been installed in a network.

8.3.3 Data maintenance

Data maintenance is another part of asset management. With the collection of large amounts of data via IoT devices, it is essential to have processes in place to maintain the data as described below.

a) Ongoing monitoring of data assets

You need to monitor the effectiveness of your IoT data collection and use. If the business purpose for your IoT data collection changes or expands, you will need to revisit your privacy, security and data governance approaches. Ensure these are monitored to maintain the ongoing efficiency and good management of your IoT approaches.

b) Data validation

Undertake data validation based on the requirements identified in your [data needs assessment](#). Where possible, data validation should be automated, and errors corrected at source. Data validation can also include the detection and mitigation of malicious data.

c) Data retention and destruction

Make sure that any legal or business requirements applying to IoT data have been implemented and that data is kept or destroyed as required. There must be appropriate retention and destruction of data generated from IoT-enabled projects in accordance with your organisation's records and information management requirements.

For data that is no longer required, delete or dispose of it at a set frequency, in accordance with requirements under the [State Records Act 1998 \(NSW\)](#), [Privacy and Personal Information Protection Act 1998 \(NSW\)](#) and [Health Records and Information Privacy Act 2002 \(NSW\)](#).

For more advice on IoT-related data retention and destruction, contact the [State Archives and Records Authority](#).

9. Assess

Best practice considerations at this stage in a project

- What have you learnt from using IoT? What will you do differently next time?
- Have you begun to realise the benefits of IoT?
- Will you change your business practices? What new things or ways of working will you implement?
- Is the business case still valid?
- To what extent was the entirety of the intended scope delivered and is there any further scope required to support the achievement of the service need?
- Has there been a review of how well the project was managed?
- Are the user needs and business needs being reviewed and the benefits being tracked?
- What evidence shows the required systems changes/transformation (technology, interoperability, processes or procedures) have been fully implemented and successfully contributed to the realisation of benefits?
- Is the project still aligned with government priorities and service need? If circumstances have changed, what is being done to ensure that the project realigns to current government priorities/service need?
- Are there opportunities in operations to enhance sustainability across the social, environmental and economic domains?
- What are the lessons learned to improve future projects, and are they being proactively collected, documented and shared to facilitate knowledge transfer?

9.1 Evaluation

Learning from your project and applying the lessons in your next IoT-enabled project is critical. This chapter provides you with practical steps on how to evaluate your project, assess whether it has met or exceeded its economic evaluations. It also contains useful evaluation resources.

9.1.1 Why is evaluation important for IoT-enabled projects?

Evaluation is the assessment of a program, process, project, product or similar (referred to as 'project' for the purposes of this chapter) to judge its effectiveness, efficiency, appropriateness, and sustainability.

Evaluation plays a key role in supporting project decision making by helping you to understand whether a project is working or not, in what context, and why.

Evaluation is particularly important for IoT-enabled projects because the technology is so new and processes of designing and implementing solutions are relatively untested. Evaluation findings can be used to:

- identify areas to improve the project
- justify the continuation or discontinuation of a project
- make a case for expansion of a project – this is important when evaluating a pilot or trial IoT-enabled project to see if it should be expanded.

9.1.2 What to evaluate

There are often three types of evaluation for a project: outcome evaluation, process evaluation, and economic evaluation. The type of evaluation conducted will determine the questions you need to ask and the content to evaluate.

All three types of evaluation are relevant for IoT-enabled projects, and the type(s) you choose to conduct will depend on what you want to discover and achieve through the evaluation. They are explained below.

a) Outcome evaluation

An outcome evaluation seeks to verify a causal link between pre-defined project activities and outcomes. Ideally, it may also identify who the program works best for and under what circumstances. It is best used when a project has been running long enough to produce reliable results. It asks questions such as:

- Have the outcomes changed?
- Has this project contributed to the change as expected?
- Who has benefited from the project, how, and under what circumstances? Who else has benefited or may benefit from the use of the data that this project has shared?
- Are there any unintended consequences for participants or stakeholders?

- Are there any unforeseen benefits for participants or stakeholders?

b) Process evaluation

A process evaluation looks at how a project is delivered, describing the project's current operating conditions and identifying processes hindering success. If conducted early, it can ensure a project is implemented as intended. If conducted as an ongoing evaluative strategy, it can be used to continually improve projects by informing adjustments to service delivery.

A process evaluation asks questions such as:

- Have the project activities been implemented as intended?
- Are there any barriers to program delivery? If so, how can the project be improved?
- Was the project implemented within the expected timeframe?
- To what extent is the project reaching intended recipients? For IoT-enabled projects, this might mean to what extent is the IoT program reaching or making a difference to the end-user and/or citizen?
- To what extent is the project meeting the needs of participants and other key stakeholders?

c) Economic evaluation

Economic evaluation identifies, measures and values a project's economic costs and benefits. It can inform decision-making and promote efficient resource allocation. It can also be used to compare alternatives on a consistent basis. The two main forms of economic evaluation are:

- *Cost-benefit Analysis (CBA)*: This involves the consistent valuation of costs and benefits in monetary terms for both monetary and non-monetary variables (remember to consider the value of data to your project and potential future projects). Further information on CBAs and how to conduct one for IoT-enabled projects is provided in [Chapter 4.2 Cost-benefit analysis](#).
- *Cost Effectiveness Analysis (CEA)*: This is used when the benefits of a program cannot be easily quantified in monetary terms, or where benefits are considered to be similar for alternative programs.

9.1.3 How to evaluate IoT-enabled projects

The process for evaluating an IoT-enabled project is the same as the process for evaluating other NSW Government programs and should follow the guidance provided by the [NSW Treasury Centre for Program Evaluation](#). The process is broadly outlined below.

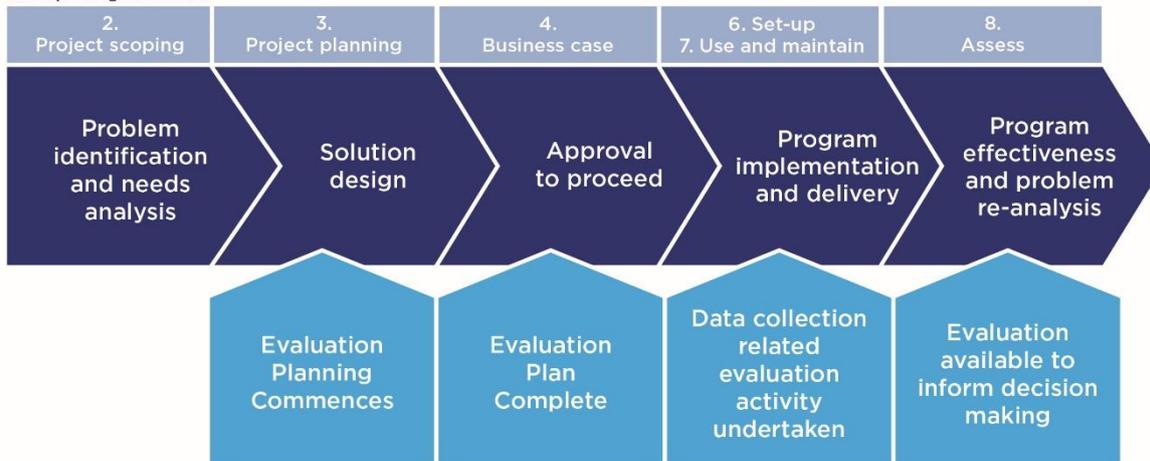
a) Planning your evaluation

Evaluation planning should start when the project is being designed, with much of the planning complete before the project has started to operate. Integrating evaluation with the project's lifecycle enables a stronger evaluation to be delivered in time to support decision-making.

The evaluation process along with the project or program lifecycle

PROGRAM CYCLE

Corresponding IoT module



EVALUATION PROCESS

Selecting and implementing an appropriate evaluation methodology requires the skills of a suitably qualified and experienced research or evaluation specialist. Speak to your organisation's Program Evaluation team, and see the [Evaluation Toolkit](#) for assistance on developing evaluation plans. The below table sets out key steps in evaluation planning.

Key steps in evaluation planning

Step	Examples of things to consider
1) Specify the subject of the evaluation	<ul style="list-style-type: none"> Are you evaluating your entire IoT-enabled project, or an element of the IoT-enabled project, e.g.: <ul style="list-style-type: none"> the technology (sensors, communications networks, platform, and analytics) functionality (including alarm/event management, device management, visualisation, performance).
2) Understand the purpose of the evaluation	<ul style="list-style-type: none"> What decisions need to be made about your IoT-enabled project? Will decision-makers be considering the project's future, including continuing, expanding or discontinuing the project?
3) Know the primary audience	<ul style="list-style-type: none"> Who will receive and use the evaluation findings?
4) Governance and oversight	<ul style="list-style-type: none"> Are effective governance processes in place?
5) Allocate and understand key roles and responsibilities	<ul style="list-style-type: none"> Who is commissioning the evaluation? Who will manage it?

Step	Examples of things to consider
	<ul style="list-style-type: none"> • Who will conduct it? • Who will be responsible for the consideration and implementation of findings?
6) Identify key questions	<ul style="list-style-type: none"> • What are the key questions the evaluation should answer? Questions could include: <ul style="list-style-type: none"> ○ Did you see the improvement you expected to see? ○ Did you discover something entirely new? ○ Did the project miss the mark?
7) Select your methodology	<ul style="list-style-type: none"> • What methodology will the evaluation use? <ul style="list-style-type: none"> ○ Typically, more than one is needed. Compare your analytics with reality by speaking with employees about their experiences with the project.
8) Disseminate the findings	<ul style="list-style-type: none"> • How will you communicate the findings to decision-makers, service providers, other stakeholders and the community?
9) Protect privacy and uphold ethics	<ul style="list-style-type: none"> • What ethical issues need to be considered and addressed?
10) Resources	<ul style="list-style-type: none"> • How much time is available to conduct the evaluation? • What is the evaluation budget? • What skills are required and available? What materials and evidence are required? • What are the key milestones and deliverables for the evaluation?
11) Include stakeholders	<ul style="list-style-type: none"> • Who are the evaluation stakeholders and how can they be included in planning, conducting and understand the evaluation findings? <ul style="list-style-type: none"> ○ Evaluation is strengthened with the active participation of project managers, staff and stakeholders.

b) Commissioning a third-party vs internal evaluation

In deciding whether to conduct an evaluation internally (e.g. through an internal evaluation unit) or through an evaluation provider (e.g. from the private sector or a university), consider:

- *Priority:* Projects can be prioritised based on their size, strategic significance and degree of risk. Lower priority projects are often more suited to internal evaluations, whereas high priority projects often require the commissioning of an independent third-party.

- *Expertise:* Think about the technical or professional skills required, and whether they are available internally or externally.
- *Independence:* An external evaluator can contribute to the independence of the evaluation.
- *Resourcing:* Commissioning can bring additional resources required to ensure timely delivery.

For assistance in determining whether to commission an evaluation or conduct it internally, see the [Program Evaluation Guidelines](#) and speak to your organisation's Program Evaluation team.

c) Using evaluation findings

Project evaluation should always be undertaken with a view to informing decision-making, such as continuing, expanding, ceasing or refining a project. For example, evaluation results can be used to support the expansion of your IoT-enabled project.

A process for responding to evaluation findings should be developed in advance of the evaluation. This needs to be embedded within the established evaluation and project governance processes.

9.1.4 Other assessment activities

Evaluation is part of a spectrum of other activities used to collect evidence and assess the project. These activities can support project evaluation and produce valuable information in their own right. They include:

- *Project reviews:* Typically, quicker, more operational assessments of "how we are going" often to inform continuous improvement.
- *Monitoring:* A management process to periodically report against planned project targets or KPIs, usually focussed on project outputs.
- *Research:* Closely related to evaluation but can ask different types of questions that may not be related to the merit or value of a project.

9.1.5 Policy and resources

For information on evaluation in the NSW Government, see the [Department of Premier and Cabinet's evaluation webpage](#). A summary of the relevant policies and resources is in the following table. While these have been developed for the NSW Government, they may also be useful for local government.

Evaluation resources

Resource/ policy	Description
NSW Treasury Centre for Program Evaluation	<ul style="list-style-type: none"> • Conducts evaluations of large and significant NSW Government programs (including process, outcome and economic components) • Leads evaluation practice across NSW, in accordance with TC18-03 Program Evaluation • Builds evaluation capability across the sector • Resources developed in partnership with other clusters include the Program Evaluation Guidelines and the Evaluation Toolkit • For more information about the Centre for Program evaluation or implementing the Evaluation Toolkit, contact evaluation@treasury.nsw.gov.au.
NSW Treasury Circular TC18-03 Program Evaluation	<ul style="list-style-type: none"> • Sets out the overarching requirements for the evaluation of existing and new programs by NSW Government.
NSW Government Program Evaluation Guidelines (2016)	<ul style="list-style-type: none"> • Developed to assist NSW Government agencies to conduct consistent, transparent and high-quality evaluations of NSW Government funded programs • All NSW Government departments should conduct their evaluations in line with the principles and standards outlined in these Guidelines
NSW Evaluation Toolkit	<ul style="list-style-type: none"> • Toolkit that accompanies the Program Evaluation Guidelines.

Auditing

Auditing or post-implementation review is an important part of project and program evaluation. It is closely linked to the evaluation of projects (see [Chapter 8.1 Evaluation](#)) and assurance (see [Chapter 3.9 Assurance](#)).

The NSW Government has an [Internal Audit and Risk Management Policy for the NSW Public Sector](#), which was created to assist agencies meet their legislative obligations. The policy strengthens internal audit, risk management, and governance practices so that projects and agencies have effective controls in place to ensure resources are used wisely.

Your organisation's Chief Audit Executive, Risk Officer or Internal Audit team can provide more information about audit.

9.1.6 Why is auditing important for IoT-enabled projects?

Since IoT is a relatively new technology, ensuring that projects are audited and reviewed on a regular basis can lead to better future rollout and should be done as a matter of good practice. Audits, whilst daunting, can lead to process and procurement improvements for future projects.

As most IoT-enabled projects are ongoing and include ongoing capture of data, be aware that a project may continue to be in operation even while being audited.

9.1.7 Document management and record-keeping

Sound document management is vital to post-project review, audit, and evaluation. Making accurate and detailed records and ensuring documents are kept are essential.

If you are using post it notes in an agile environment, consider the implications under the [State Records Act 1998 \(NSW\)](#) and any relevant records policies. Refer to the [State Archives & Records](#) and [Information and Privacy Commission NSW](#) for information about government recordkeeping.

9.1.8 The NSW Audit Office

The NSW Audit Office is the statutory authority that conducts audits for the Auditor General. The NSW Audit Office conducts two types of audits for both NSW Agencies and local governments:

- *Performance audits*: Performed on programs or individual projects to review whether they are carried out efficiently, effectively, economically and in accordance with relevant laws.
- *Financial audits*: Provide independent opinions on the financial statements of NSW government entities, universities, and councils.

10. Appendices

Appendix A – Pre-mortem exercise

What is a pre-mortem?

A pre-mortem is a group brainstorming exercise where the group plays ‘devil’s advocate’ to critique plans and projects. The purpose is to identify vulnerabilities in a project and develop specific actions to mitigate, avoid, transfer or accept risk before it is too late.

This exercise brings forward the post-mortem so that a project can be improved at the start, rather than autopsied at the end.

Pre-mortems are ideally conducted early in a project, but they can be conducted at any time and repeated as often as required.



Tip: This exercise is particularly useful for projects involving IoT due to the rapidly-evolving IoT industry and the breadth of risks associated with IoT and data.

Benefits of a pre-mortem

The pre-mortem exercise helps overcome blind spots and optimism bias by reframing a project as a failure. It helps the project team to recognise warning signs faster, and bridges short-term and long term thinking so that risks can be mitigated.

The pre-mortem encourages creative thinking and foresight by:

- Generating more ideas by focusing on the prospective hindsight of “what did go wrong” rather than the typical foresight of “what could go wrong”
- Encouraging those who are usually quiet to speak up because ideas are generated anonymously
- Rewarding people for being imaginative in finding flaws in a project.

Steps in conducting a pre-mortem

Step	Description	Suggested time
1	<p>Group is briefed on the project (recommend including people with a stake in the project such as the project sponsor, subject matter experts, external critics).</p> <p> <i>Tip: You may wish to invite an organisation which has previous experience with your kind of project or the subject matter. The more varied the participants, the better– you will generate more ideas and the transparency of the process can assist with getting project buy-in.</i></p>	5 minutes
2	<p>Group chooses a date in the future and imagines that the project has failed.</p> <p> <i>Tip: Play with different failure scenarios. Different failure scenarios will raise different themes.</i></p>	5 minutes
3	<p>Individually, group members write down every reason they can think of for the project's failure, with as much detail as possible, without fear of being impolite.</p> <p>This can be done with sticky notes or in a Google Document.</p> <p>Questions to think about can include:</p> <ul style="list-style-type: none"> • What went wrong and what were the possible causes? • Were there warning signs? 	10 minutes
4	<p>The group discusses the identified reasons for the project failure by theme:</p> <ul style="list-style-type: none"> • What are the themes? • What is within the team's control? 	40 minutes
5	<p>For each identified reason for failure, consider what actions could be taken to mitigate that risk, and where possible, build the action into the project.</p> <p>You can follow this exercise by identifying any red flags which, should they occur, could prompt action:</p> <ul style="list-style-type: none"> • What are the actions? • Who is responsible for doing what? • What are the red flags to prompt action? <p> <i>Tip: The clearer and more granular you can be, the better. If possible, add the name of the person or position responsible, so that accountability is clear.</i></p> <p><i>Once you have finished step 5, do not file the results away to be forgotten about. Keep your Risk Register up to date and do not be afraid to repeat this pre-mortem exercise at various points during your project.</i></p>	As much time as required

Example pre-mortem exercise

Step	Issue	Brainstorming
1	Project brief	We want to install smart street lights that turn on when motion is detected on the street. Stakeholders include the project sponsor, the team who will manage the lights and the general public.
2	Fast forward to the future	One year later... failure. The lights have to be uninstalled and the project is cancelled. The public was angry that data was being collected about their movements and sold by the supplier of the sensors to third parties.
3	What went wrong and why?	<ul style="list-style-type: none"> We did not check that data collected would not be owned or accessible to the sensor supplier – <i>“We were not sure if data would be collected...”</i> We did not engage with the general public sufficiently during the process to hear and understand their concerns – <i>“We did not have time to engage with the public more...”</i> We did not adequately plan stakeholder engagement – <i>“We thought engaging with the project sponsor and releasing an announcement would be enough, we have never done a communications stakeholder plan...”</i> We missed critical steps in the procurement process – <i>“We did not think about the data when procuring sensors, we had no example to follow, we did not know who to talk to as a sounding board, we did not have procurement experience, we did not do due diligence...”</i>
	Were there warning signs?	<ul style="list-style-type: none"> The IoT service provider did not specify who would own the data collected – <i>“We assumed we would own the data...”</i> There was previous discontent from the public around smart technology, including smart bins – <i>“We did not think people would care about smart lighting data being collected...”</i>
4	Themes	<ul style="list-style-type: none"> Data collection Data ownership Stakeholder engagement Expertise within the project team.
	What is in our control?	All of the themes above.
5	What actions can we take to avoid failure?	<ul style="list-style-type: none"> Include a clause in our contract with the IoT service provider which stipulates that data is owned by the user (NSW Government). Engage the public by developing a process map that specifies who needs to be contacted and when and why. Review it weekly. Create a register of feedback and complaints to be monitored throughout the project, to detect warning signs and discontent.
	Who is responsible for doing what?	<ul style="list-style-type: none"> Project team and procurement team - responsible for data ownership in the contract. Project sponsor and project manager - responsible for citizen engagement.
	Are there red flags?	<ul style="list-style-type: none"> IoT service providers do not respond to questions about data ownership.

Appendix B – Privacy Collection Statement template

We are [Insert, e.g. The Office of Widgets]

The [Office of Widgets] is part of the [NSW Department of Things]. We [make widgets].

What personal information are we collecting?

We are collecting information about [the kinds of widgets you use], including [how many times you use widgets, and where you use them].

How are we collecting your personal information?

We collect information [when you use our widgets. Our widgets are connected to the internet, and collect data when they are used].

Why are we collecting your information?

We are collecting your personal information so we can [assess how many widgets we need to provide, and where we should provide them]. We may also use this information to [conduct research about things], or [deliver better thing services].

[If applicable: We are required by law to collect this information].

If we do not collect this information, we will not be able to [provide you with information about your widgets]. You can read more about [our widget program] here: [link to more information].

What will we do with the information?

We will use the information you give us to [deliver our widget program, and conduct thing research].

[If applicable: We share the information we collect with [the Department of Boxes] to [help them plan their widgets in boxes program]].

We will keep your information for [X years]. After that time we will securely [destroy/de-identify it]. We may keep de-identified or aggregated records indefinitely.

Access and correction

You can access any information we hold about you and ask us to correct it if it is wrong. If you would like to do this, please contact us. Our contact details are set out below.

Contact us

Our address is [Level 1, 123 Australia Street NSW 2000]. You can call us at [1800 555 555]. You can write to us at [widgets@things.nsw.gov.au] or at [postal address].

Privacy Policy

You can read our privacy policy here: [insert link]. Our privacy policy has more detail on how we handle personal information, including how you can make a complaint.

Appendix C – Checklist for IoT solutions

- Assess your requirements around performance, business continuity and back up to design your IoT Hub and Edge and determine the level of intelligence they require
- Carefully consider if the solution is fit for purpose, by looking at:
 - what you want to achieve with the IoT solution
 - the operational context of your organisation
 - what you need in a Minimum Viable Product.
- Do not use IoT solutions which do not comply with Australian regulatory requirements
- Look for IoT solutions which voluntarily adhere to standards, and open systems/ standards/source to avoid vendor lock-in
- Use Device Detection Capability if available to save time
- Undertake a security and data privacy assessment to determine the appropriate level of security and data privacy the IoT solution should provide
- Consider your network needs including range, power consumption, and bandwidth, for now and into the future (e.g. in five years), noting that all IoT networks may be currently available in your location
- If using a proprietary network, check with the network provider if your device is compatible with the network
- Avoid vulnerable devices and choose devices that can be managed, monitored and maintained at a component level
- Verify that firmware can be updated remotely
- Check if your preferred sensors are available and supported in Australia, suitable for your environment, and field-proven for the application you require
- Consider the capability of battery solutions, including battery life and power consumption
- Positioning devices must record spatial data to be absorbed into the NSW Digital Twin
- Consider what level of automation is appropriate and if it can be customised
- Understand the functionality available via your API and use open APIs where suitable
- Consider risk mitigation strategies such as using separate servers or networks for data exposed through APIs
- Describe datasets or data sources using open standards and persistent identifiers (long-lasting references of URLs).

Appendix D – Key IoT wireless network options currently available in NSW

	Low-Power Wide-Area Network (LPWAN)				Cellular network		Local/Personal Area Network (LAN/PAN)		
Range	High				High		Low		
Bandwidth	Low				High		High		
Power use	Low				High		Low		
Features	<ul style="list-style-type: none"> ✓ Suited to connected devices which require long-range transmission, low power consumption, long battery life, e.g. industrial applications that require devices to continuously transmit small amounts of data over great distances for many years on a single battery ✓ Suited to rural and remote locations ✓ IoT applications include asset tracking, smart cities, agricultural and environmental monitoring and sensors ✗ Not suited to applications requiring high data transmission 				<ul style="list-style-type: none"> ✓ Can transmit lots of data ✓ Can use if the device is in cell tower range ✗ Not ideal for battery-powered IoT devices e.g. sensors 		<ul style="list-style-type: none"> ✓ IoT applications include consumer applications, building automation, in-house energy management ✗ Low coverage, not scalable ✗ Wireless LANs may have licensing requirements 		
Examples	<p>Sigfox</p> <p>Proprietary technology: Devices must be registered on the Sigfox portal and a subscription fee paid. ThinXtra manages the network in Australia. Sigfox is also an end-to-end service where the functions and features available are those determined by Sigfox. Not ideal if device control is necessary.</p> <p>Devices should be certified RCZ4 (ANATEL 506, AS/NZS 4268) for use in Australia.</p>	<p>LoRaWAN</p> <p>LoRaWAN is an open standard. Users can manufacture LoRaWAN base stations and devices add their own gateways to the network, and/or install and operate a LoRaWAN network for free.</p> <p>Network can be public (e.g. NNNCo is Australia's LoRaWAN network operator) or users can build and operate a private LoRaWAN network.</p> <p>In Australia, AU915 or AS923 band plans are supported.</p>	<p>Narrowband IoT (NB-IoT)</p> <p>Extended coverage via existing cellular networks. Managed by major telecommunications carriers: Telstra, Optus, Vodafone. Carriers have control of the devices that use their spectrum.</p> <p>Suited to very low data rate applications in extremely challenging radio conditions.</p> <p>Less expensive than Cat-M1.</p>	<p>LTE Cat-M1</p> <p>Extended coverage via existing cellular networks. Managed by major telecommunications carriers: Telstra, Optus, Vodafone. Carriers have control of the devices that use their spectrum.</p> <p>Higher data transmission without interruptions and more accurate device positioning than NB-IoT. Good for sensors on moving devices.</p>	<p>4g</p> <p>Useful for high-bandwidth applications where there is a direct power source (or regular battery charging), limited number of devices, in populated areas.</p>	<p>5G</p> <p>5G coverage across NSW is limited, not yet available in regional areas.</p> <p>Currently delivered by Telstra. Optus and Vodafone are set to follow.</p>	<p>ZigBee</p> <p>Compared to Wi-Fi, lower power consumption but also slower. ZigBee is often controlled by a specialised device rather than via smartphone.</p>	<p>Wi-Fi</p> <p>Wi-Fi controlled smart devices tend to be more expensive than ZigBee controlled devices. Relatively power-hungry compared to ZigBee or Bluetooth.</p>	<p>Bluetooth</p> <p>Users can only affect control of the smart device from a relatively close range.</p> <p>Economical as virtually every smartphone is Bluetooth enabled.</p>

Useful links for wireless network options

- [The Things Network](#)
- [Sigfox](#)
- [Thinextra](#)
- [Lora Alliance](#)
- [NNN Co](#)
- [Wireless LAN licensing requirements](#)
- Telecommunications carriers may publish maps of IoT networks they provide (e.g. NB-IoT and Cat-M1) and/or a list of integrated devices for use with their networks. For example, Telstra has published a [Telstra IoT network coverage map](#) and a [list of certified devices](#) for its network.

Appendix E – The Five Safes

The 'Five Safes' is an internationally recognised risk management model that can help you identify and manage data sharing risks. Under this framework, data sharing risks are managed across five 'safety' dimensions.

For each of the safe dimensions, there are a set of questions that you should ask the data requestor to help you identify and manage any risks. You can do this by asking them to complete a data sharing request/access form or by having a conversation with them directly.

For detailed guidance on applying the five safes, refer to the [Australian Government Best Practice Guide to Applying Data Sharing Principles](#).

Safe dimension	Questions to ask the data requestor
<p>Safe People</p> <p>The knowledge, skills, incentives of the users to store and use the data appropriately.</p>	<p>Rationale: The individual/s or organisation/s receiving the data must be an appropriate recipient:</p> <ul style="list-style-type: none"> • Are they appropriately equipped and do they possess the relevant skills and experience to effectively use the data for the proposed purpose? • Will they restrict data access to only specified persons with the appropriate security clearance/s? • Can they or will they engage with the organisation providing the information to support the use of the data for the proposed purpose? • Are other persons or bodies in addition to the data recipient invested in the outputs of the project and the motivations of those persons or bodies?
<p>Safe Settings</p> <p>The practical controls on the way the data is accessed.</p>	<p>Rationale: The environment in which the data will be stored, accessed and used by the individual/s or organisation/s receiving the data must be appropriate:</p> <ul style="list-style-type: none"> • Is the physical location where the data will be stored and used appropriately? • Is the location of any linked data sets appropriate? • Does the organisation receiving the data have appropriate security/technical safeguards to keep data secure and prevent unauthorised access and use? • What is the likelihood of deliberate or accidental disclosure or use occurring? • How will data be handled after it has been used/shared for the specified purpose?
<p>Safe Projects</p> <p>The legal, moral, and ethical considerations surrounding</p>	<p>Rationale: The purpose for which data is to be shared and used must be appropriate.</p> <ul style="list-style-type: none"> • What is the proposed use of the data and is the data necessary for that purpose? • Will the purpose of the data sharing or use be of value to the public?

<p>the use of the data.</p>	<ul style="list-style-type: none"> • Does positive public interest outweigh negative public interest? • Is there a risk of loss, harm, or other detriments to the community if the sharing and/or use of the data does not occur?
<p>Safe Outputs The residual risk in publications from sensitive data.</p>	<p>Rationale: The publication or other disclosure of the results of data analytics work conducted on data shared under the <i>Privacy and Personal Information Protection Act 1998</i> (NSW) must be appropriate:</p> <ul style="list-style-type: none"> • What is the nature of the proposed publication or disclosure? • Who is the likely audience of the publication or disclosure? • What is the likelihood or extent to which the publication or disclosure may contribute to the identification of a person to whom the data relates? • Will the results of the data analytics work or other data for publication or disclosure be audited and/or will that process involve the provider organisation?
<p>Safe Data The potential for identification in the data, as well as its quality and sensitivity.</p>	<p>Rationale: The purpose for which data is to be shared and used must be appropriate:</p> <ul style="list-style-type: none"> • What is the proposed use of the data and is the data necessary for the purpose? • Will the purpose of the data sharing or use be of value to the public?

Appendix F – NSW Government policy, framework or tool referenced in the IoT Policy

NSW Government policy, framework or tool	IoT Policy chapter
Preparing for effective engagement: A guide to developing engagement plans (2012)	3.2 Stakeholder engagement
NSW Government Information Classification, Labelling and Handling Guidelines	3.3 Data needs assessment 3.7 Data obligations
NSW Government Cloud Policy (2018)	3.3 Data needs assessment 3.4 Risks and Obligations
Internal Audit and Risk Management Policy for the NSW Public Sector (2015)	3.4 Risks and Obligations
NSW Auditor General's report - Internal Controls and Governance (2018)	3.4 Risks and Obligations
Audit Office of NSW Risk Management Framework (2018)	3.4 Risks and Obligations
NSW Treasury Risk Management Toolkit (2012)	3.4 Risks and Obligations
NSW Cyber Security Policy (2019)	3.4 Risks and Obligations 3.6 Cyber Security
NSW Government Procurement Guidelines - Risk Management (2006)	3.4 Risks and Obligations
NSW Data and Information Custodianship Policy (2013)	3.4 Risks and Obligations
SafeWork NSW codes of practice	3.4 Risks and Obligations
Information Governance Agency Self-Assessment Tools	3.5 Privacy
Guide to Privacy Impact Assessments in NSW	3.5 Privacy
NSW Open Data Policy	3.7 Data obligations 7.2 Data sharing
NSW Gateway Policy	3.9 Assurance
ICT Assurance Framework	3.9 Assurance
Infrastructure Investment Assurance Framework	3.9 Assurance
Recurrent Expenditure Assurance Framework	3.9 Assurance
NSW Government Business Case Guidelines	4.1 Business case
Infrastructure NSW Business Case Toolkit	4.1 Business case
NSW Government Guide to Cost-Benefit Analysis (TPP 17-03)	4.2 Cost-benefit analysis

NSW Government policy, framework or tool	IoT Policy chapter
NSW Government Benefits Realisation Management Framework	4.2 Cost-benefit analysis
NSW Procurement Policy Framework	5.1 Procuring IoT solutions
NSW Procurement Board Directions	5.1 Procuring IoT solutions
NSW Government Small and Medium Enterprise and Regional Procurement Policy	5.1 Procuring IoT solutions
Procurement Risk Register	5.1 Procuring IoT solutions
NSW Procurement Board Industry Engagement Guide	5.1 Procuring IoT solutions
Procurement Strategy template	5.1 Procuring IoT solutions
NSW Standard for Spatially Enabling Information (2018)	6.2 Spatial data requirements
Data Quality Tool	7.2 Data sharing
Total Asset Management Guideline: Asset Maintenance Strategic Planning (TAM06-3)	7.3 Asset, device and data management
Evaluation Toolkit	8.1 Evaluation
NSW Government Program Evaluation Guidelines	8.1 Evaluation'
Smart Infrastructure Policy	1.2.3. Existing policies and strategies
Smart Places Strategy	1.2.3 Existing policies and strategies

11. Document Control

11.1 Document Approval

Name & Position	Signature	Date
Dawn Routledge Executive Director, Office of the Secretary		Version 1.0: 15 October 19
Glenn King Secretary		Version 1.0: 15 October 19

11.2 Document Version Control

Version	Status	Date	Prepared By	Comments
1.0	Final	09 Sep 2019	Strategy & Policy, Office of the Secretary	
1.1	Final	1 February 2020	Strategy and Policy, Office of the Secretary	Minor amendments made. New and updated standards have been added.
1.2	Draft	02 March 2021	Strategy and Policy, Office of the Secretary	Annual refresh of the policy. Amendments made to reflect updated standards, case studies and new information available.