

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:

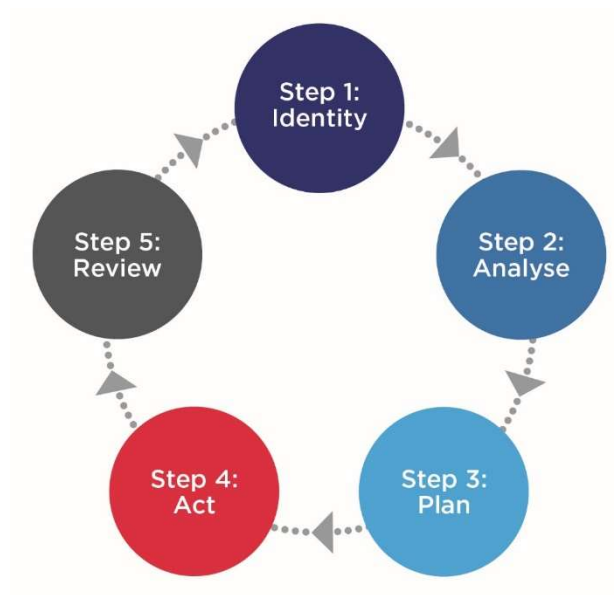
- does not meet its intended purpose
- is actively opposed
- does not integrate with existing systems
- breaches legislation or regulations
- increases business processes
- creates a negative user experience.

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



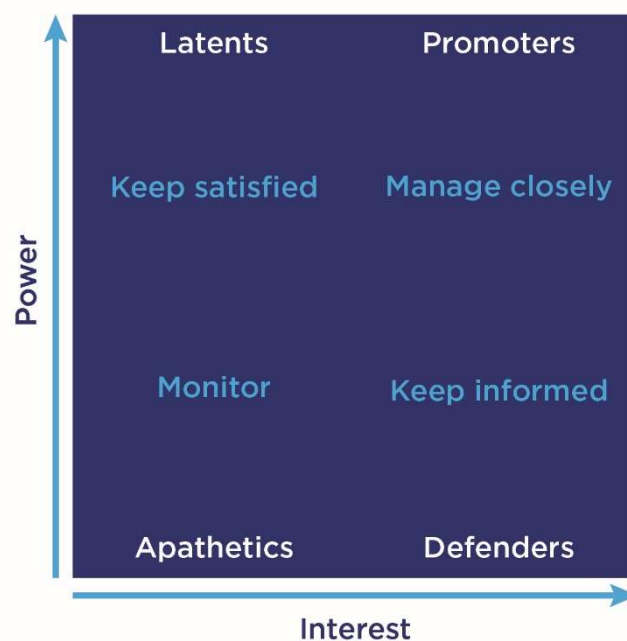
2) Analyse your stakeholders

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.

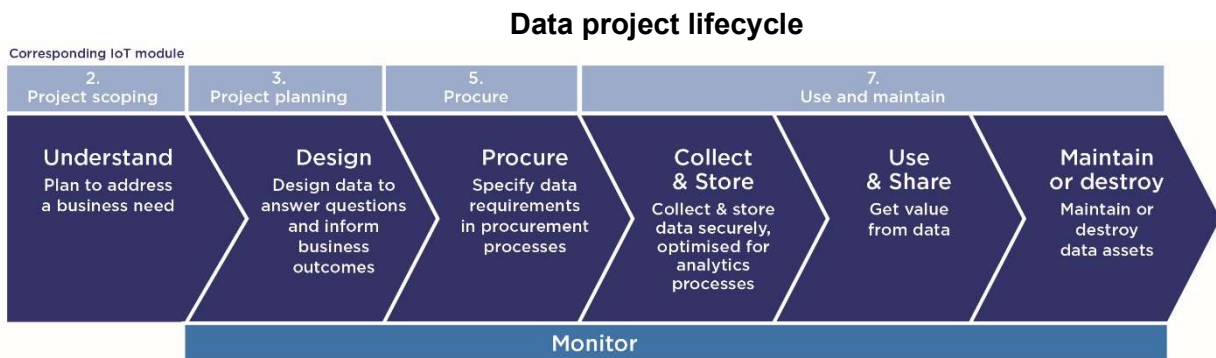
The resident argued that by requiring individuals to enter their licence details, their personal information was being collected and could identify them.

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 Compliance 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	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: <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	Specifies: <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?

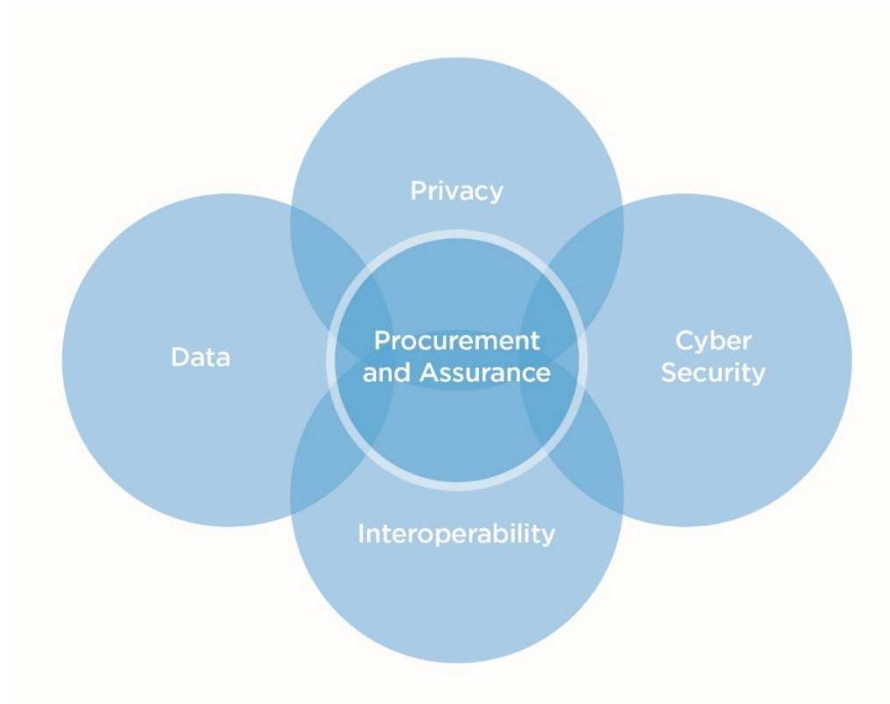
Assurance is the process of providing independent confidence for projects. Assurance involves regularly examining a project against an approved business plan and what it was intended to do, or service needs it was intended to meet.

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.