8. Use and Maintain

Best practice considerations at this stage in a project

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

8.1 Data analysis and use

8.1.1 The data analytics process

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

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

Examples of types of data analytics used for IoT data

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

a) Steps for data analytics

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

- data requirements specification
- data collection
- data cleansing
- any required privacy preserving measures, such as anonymisation and deidentification
- data modelling

- data visualisation and communication.

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

1) Data cleansing

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

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

2) Data engineering and modelling

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

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

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

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

3) Visualisation and communication of data

Communication is the last step of the data analytics process and is often overlooked. Data needs to be delivered to the organisation in a meaningful way to support decision making. Data visualisation is about the visual representation of data as a means of communication. Note that licences are required for most visualisation tools.

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

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

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

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

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

b) Next steps after the data analytics process

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

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

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

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

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

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

Case Study – NSW Health's Proactive Sepsis Management project

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

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

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

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

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

The benefits of the project across stakeholder groups include:

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

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

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

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

8.1.2 Using data for your business outcomes

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

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

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

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

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

8.2 Data sharing

8.2.1 Why and how to share data

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

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

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

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

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

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

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

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

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

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

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

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

8.2.2 Responding to requests for data sharing

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

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

Steps for data sharing

Step	Description
1) Can the data be shared legally and under what conditions?	• Certain laws and regulations prevent or limit the scope of sharing some forms of data. You must consider your legal and compliance obligations with respect to whether you can share the data and under what conditions. • *Does the data requested contain personal information?* Under the *Privacy and Personal Information Protection Act (1998)* (NSW), personal information may only be used or shared for the purpose for which it was collected, or for a secondary purpose if an exception applies. You must determine whether the sharing of personal information with a third party is compatible with the original purpose it was collected for and the privacy policy and/or notice given to the individual. If it is not compatible, the data that contains personal information must be de-identified. If the data is successfully de-identified, the modified data will no longer trigger privacy legislation. Step 3 explains how to de-identify data. • *Does the requested data contain other sensitive information?* Legal restrictions prohibit the sharing of some forms of sensitive information, such as data protected by intellectual property rights, data considered confidential (including trade secrets), financial data, etc. This data cannot be shared in its raw format, except in exceptional circumstances. A decision not to share data should only be made after consultation with your organisation's legal officers and after all attempts have been made to protect the sensitivity of the data. • *Exceptions?* In some instances, the sharing of sensitive and personal information in its raw form is legally permitted, such as: ○ where the data subjects have given consent ○ where it is necessary for the performance of government duty that is in the public interest ○ where it is necessary for the purposes of the legitimate interests pursued by the organisation disclosing the data, or the party receiving it, as balanced against the rights and interests of the data subjects.

Step	Description
	• *Will the requested data be linked with one or more datasets?* Just because data does not contain sensitive information does not mean that it will not become sensitive once it is shared. Non-sensitive data may become sensitive when the data is linked with one or more datasets that include information about the same person or some subject. For example, location data, identification numbers or online identifiers, such as IP addresses, cookies, and RFID tags, can provide ways to make data personally identifiable. Talk to the data requestor about how they intend to use the data. • *No legal or compliance issues identified?* If there are no legal or compliance issues, you should consider making this data publicly available in accordance with the NSW Government Open Data Policy.
2) Is the use of the data appropriate?	• Use of data that is not appropriate may lead to poor or detrimental decisions. To determine whether the data is appropriate, consider: ○ whether the data will be used to provide a public benefit ○ whether the data requested is fit for purpose. • NSW Government agencies have a legal and ethical requirement that data may only be shared if the data satisfies a public interest purpose test. Before sharing your data, you must check with the data requestor to see if the data will be used to inform: ○ government policy ○ research and development with a public benefit ○ program design, implementation, and evaluation ○ delivery of government services. • Where appropriate, consult with relevant stakeholders on how to provide the data and ensure it is used appropriately. This means being transparent and creating opportunities for stakeholders and citizens to provide input on proposed data-sharing agreements.

Step	Description

	• You need to determine if the data requested is fit for purpose:
	  ○ As a data owner, you have the best understanding of what can and cannot be achieved with the data you hold. Speak to the data requestor about their purpose of the data use and if the data can support it. It is also best practice to attach a Data Quality Statement to the data-sharing agreement.
	  ○ If machine learning was used, document the confidence level in the processed data and share this with the end-user.

3) Is there any privacy and/or security risks that need to be managed?	• Data that does not contain sensitivities may not require extensive consideration of privacy and security risks. However, if the data contains personal information or other forms of sensitive information, the data should only be shared once privacy and security risks have been identified and managed. See chapter 3.5 Privacy for advice.
	• Managing privacy and security risks can be managed with a range of risk-management controls, including:
	  ○ Using the 'Five Safes' (an internationally recognised risk management model). Control access to the data across the 'five safe' dimensions to ensure sensitive data is protected and only used by trusted staff for approved purposes. See Appendix E for a description of the Five Safes.
	  ○ Applying disclosure control techniques to the data (e.g. removing direct identifiers or suppressing individual records)
	  ○ Providing aggregated insights instead of sharing raw data.
	• It is best practice to apply a mix of risk-management controls when sharing sensitive data. For example, IoT data can be encrypted and then stored on a cloud server which only the data requestor can access. A data-sharing agreement can also be developed to formalise the terms of access. Applying a combination of controls helps to ensure that:
	  ○ the data recipient is authorised and equipped to use and interpret the data
	  ○ the data recipient uses the data in an appropriate manner
	  ○ neither the environment the data will be stored in, nor the data output will pose risks.
	• Safeguarding techniques should only be applied to data if there is a good reason to do so. Too much tinkering with the data may result in safe but poor quality and ultimately useless information. For example, the provider of a predictive maintenance solution may want the serial number of devices, real-time error codes, and maintenance schedule for the

Step	Description
	plant. Any form of aggregation compromises the ability of the solution to function properly, Hence, de-identification and aggregation in this case are not fit for purpose.

4) Formalise the arrangement through a data-sharing agreement	• A Data Sharing Agreement (DSA) is a document between the data owner and the data recipient/s that sets out the terms and conditions of the data-sharing arrangements.
	  ○ There are many forms of data sharing agreements, some are legally enforceable, and some are not (e.g. a Memorandum of Understanding (MoU)).
	  ○ The NSW Government has an MoU template. It is best practice to make data sharing agreements publicly available to maximise transparency.
	  ○ Formally documenting the details of your sharing arrangement is a useful governance mechanism that provides transparency and clarity for all parties involved.
	• DSAs typically cover:
	  ○ what data should be made available
	  ○ who can access and (re)use the data
	  ○ what can the (re)user do with the data
	  ○ whether or not they have the right to distribute the data
	  ○ technical means of data access and transfer
	  ○ frequency of data access
	  ○ data protection/security/confidentiality obligations
	  ○ Data breach notification requirements
	  ○ Liability questions and audit rights for both parties
	  ○ duration of the agreement
	  ○ termination of the agreement

Step	Description
	○ costs (if applicable) ○ governing law and competent court. • The DSA should identify who owns the devices, data, and insights derived from the data, and who is responsible for dealing with privacy notifications. In some cases, a dataset can be a combination of several sources so it is vital that ownership is articulated and agreed upon. • Consider how your DSA can meet the specific needs of the user so that mutual benefits are realised. Consult with the data requestor to determine the most appropriate DSA.
5) Monitor compliance with the data-sharing agreement	• Monitor the agreement to verify compliance with the terms and conditions.

8.3 Asset, device and data management

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

8.3.1 Asset management

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

a) Relevance for IoT-enabled projects

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

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

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

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

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

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

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

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

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

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

c) How to manage assets and develop a maintenance plan

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

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

d) Disposal

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

8.3.2 Device maintenance

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

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

a) Hardware maintenance

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

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

b) Software maintenance

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

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

8.3.3 Data maintenance

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

a) Ongoing monitoring of data assets

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

b) Data validation

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

c) Data retention and destruction

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

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

For more advice on IoT-related data retention and destruction, contact the State Archives and Records Authority.