5. Procure

Best practice considerations at this stage in a project

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

5.1 Procuring IoT solutions

5.1.1 Procuring IoT goods and services

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

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

5.1.2 Procurement landscape

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

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

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

5.1.3 Contacts for procurement

These resources can help you on your procurement journey:

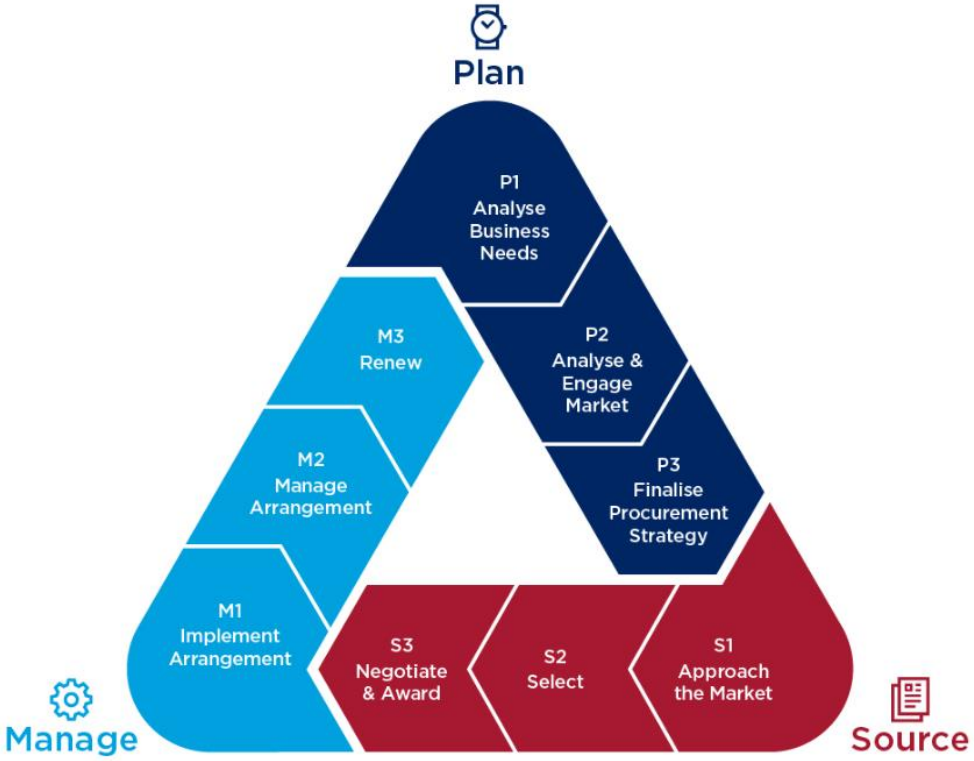
- NSW Government agencies can contact your cluster's Chief Procurement Officer for tailored advice and information on the procurement processes and resources available in your agency.
- ProcurePoint is your one stop shop for all NSW Government procurement information. It is where all whole of government procurement policy, guidance and training is published.
- The NSW Procurement Service Centre can provide general advice on whole of government procurement policy, Board Directions, whole of government contracts and prequalification schemes.
- Local councils can contact your internal procurement teams of Regional Organisations of Councils (ROCs) for procurement support.

5.1.4 How do I procure?

a) What is a best practice procurement process?

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

The three stages of procurement



b) Managing challenges in the procurement process

Key challenges in the procurement process for IoT are:

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

  Ensure your procurement process considers the whole of life costs, including any external support needed to maintain the IoT solution or service. For example, the IoT service provider may collect, store and analyse the data captured for your organisation.

- *Ensuring your procurement strategy supports industry participation*

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

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

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

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

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

5.1.5 What to do if the perfect solution does not exist

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

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

5.1.6 Designing specifications

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

Considerations when building specifications for IoT-enabled projects

Consideration	Description
Focus on outcomes and success criteria	Being clear about your desired outcome and success criteria creates opportunities to achieve the same outcome through different means. For example, if you want to improve public safety, IoT service providers can provide different solutions including smart lighting, GPS monitoring and CCTV cameras. Prescriptive specifications are used when you clearly understand your needs and the product requirements, for example, a decision has been made to procure smart

Consideration	Description
	lighting. This narrows the diversity in IoT service provider responses.
Network needs	You need to think about what sort of network connectivity is required. For example, will your IoT device need to be accessible through public internet or a private network? See Chapter 3.8 Technology for IoT for network options.
Asset maintenance, asset onboarding and management	Understanding how a device will be installed, how often and how easily it can be updated, and the availability of replacement parts can help your future-proof your IoT solution. Also think about maintenance requirements for the broader IoT ecosystem (i.e. how do the maintenance needs of your IoT solution align with other IoT devices used by your organisation). See also Chapter 3.8 Technology for IoT and Chapter 7.3 Device and data maintenance.
Designing your IoT architecture	To design your IoT Hub and Edge, you need to consider your requirements around performance, business continuity and back up. See Chapter 3.8 Technology for IoT for guidance.
Sensor positioning data	Sensors that will (or have the potential to) feed into the NSW Digital Twin must record the device location and a time and data stamp in accordance with the requirements set out in Chapter 6.2 Spatial data requirements chapter.
Scalability	Consider if the current scope/use of the IoT solution may be expanded in future. For example, if it is a pilot, it may be used in other locations or across NSW if successful.
Interoperability	Interoperability is complex as IoT supports many applications across different industries and disciplines. You need to understand the existing technology systems in place that may be affect the IoT solution's ability to achieve the desired outcome. Your IT department is the best source of information. See also Chapter 3.8 Technology for IoT for more on interoperability.
Open source versus proprietary systems	Open source systems are fundamental to interoperability. You should choose open technology where available to avoid vendor lock-in. Similarly, you may be able to find IoT service providers who try to solve for interoperability by offering solutions compatible with proprietary protocols.
Privacy and personal information	Do not collect personal information unless absolutely required. Data collected using sensor networks may be personal information if it is about an identified person or can

Consideration	Description
	'reasonably' be linked to an identified person. See also Chapter 3.5 Privacy.
Relevant standards	Investigate if there are any standards instruments that are applicable. These may be international, national, or specific to your organisation. Chapter 3.8 Technology for IoT lists standards related to IoT, devices and equipment.
Cyber security	IoT devices are inherently insecure. You should embed cyber-related risks into your procurement business case. See Chapter 3.6 Cyber security for a list of vulnerabilities.
Data requirements	Specifications should include: • data requirements, including adherence to data standards and data quality requirements • privacy and information security requirements, including adherence to legislation and government policy • data breach and security incident notification and management processes • data quality requirements • data ownership and rights, including for data assets generated from multiple sources • data retention and disposal requirements, including when the contract ceases or is terminated • data storage requirements, including data sovereignty • legislative compliance requirements, including the *Privacy and Personal Information Protection Act 1998* (NSW), *Health Records and Information Privacy Act 2002* (NSW), *Government Information (Public Access) Act 2009* (NSW), *State Records Act 1998* (NSW). See also Chapter 5.2 Data considerations for contracting.
Indemnities	Indemnities support insurances in managing contract risks, and should be appropriate to the size and risk of the investment. NSW Government agencies are required to cap indemnity given by a service provider, which is determined based on the goods or services involved. More information is available at ProcurePoint.
Insurance	You need to consider: • the level of public liability required (taking into account the risk profile of the procurement and products or services)

Consideration	Description
	• if professional and/or product insurance is required, and if so, what is the appropriate level. Unnecessarily onerous insurance requirements will increase the cost of the procurement. More information is available at ProcurePoint.
Change management	Consider the costs and impacts of transitioning from the existing state to a new system, product and IoT service provider.

5.1.7 Procurement risks

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

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

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

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

Common risks in procurement involving IoT goods and services

Procurement risk	How to avoid it
Insufficient lead-time resulting in inadequate responses from and higher prices from prospective IoT service providers	• Involve procurement officers in project planning phase. • The NSW Procurement Board Industry Engagement Guide provides advice on planning industry engagement activities and how to incorporate the outputs and outcomes into the formal procurement process.

Procurement risk	How to avoid it

Inadequate or unclear specifications that:
• result in responses which are insufficient/ do not meet your needs/are difficult to evaluate
• create the possibility that evaluation will not meet probity/ audit scrutiny
	• Seek advice from procurement officers or other teams or organisations that have experienced similar issues.
	• Have a clear understanding of the problem you are trying to solve/outcome you want to achieve and your success criteria.
	• Run a multi-stage tender process where you:
	  ○ release specifications for industry input prior to the final tender being released
	  ○ run an information session/workshop.
	Publish these opportunities publicly (i.e. on eTendering) to give all prospective tenderers an opportunity to participate.

Misrepresentation of facts by potential IoT service providers resulting in claims of unethical or unfair dealing, or breach of contract	• Independently verify service provider qualifications. • Conduct due diligence checks such as past convictions, corruption findings, bankruptcy or insolvency checks. • Seek referee reports and independently verify their accuracy. • Confirm adequate performance if the IoT service providers has previously supplied to government.
Selection of inappropriate procurement strategy leading to an inadequate or inappropriate result and/or not achieving value for money	• Consider your business needs, key risks and opportunities. Be clear on your desired procurement outcomes. This must be reflected in your procurement strategy (check out the NSW Procurement Approach for a Procurement Strategy template). • Engage early with your procurement team and other experts. • Research the market so the procurement strategy is effective within current market dynamics. • You can also consider: ○ A collaborative or staged market approach (e.g. competitive dialogue, Expression of

Procurement risk	How to avoid it
	Interest or request for proposals) then seek tenders from the best respondents. ○ Negotiating with best performing IoT service providers to improve value for money and/or responses (your tender documents should allow you to do this). ○ Running a limited tender if it is clear that a limited number of IoT service providers can meet your requirements (following an open tender). Note there are restrictions on this if your procurement is subject to an international procurement agreement (see the International Procurement Arrangement Guidelines).
Inappropriate evaluation criteria leading to inadequate or inappropriate response, or not achieving best value	• Negotiate with the best performing IoT service providers to improve value for money and/or responses (your tender documents should allow you to do this). • Go to market again – consider using a staged procurement approach if the specifications are not clear, and revise the evaluation criteria to so that it will adequately assess the solution.
Terms and conditions are unacceptable to IoT service providers leading to higher costs, tenders with numerous qualifications/exemptions, or no/limited number of tender responses	• Use standard terms and conditions (where they exist) or develop commercially accepted terms that are tested with the market. Avoid onerous reporting requirements, short delivery timeframes or departure from industry standards. • Do not try to contract out of all risks. Best practice is to allocate risks based on who is best placed to manage them. Do not ask IoT service providers to carry a risk that is outside their control.
Actual or perceived breach of confidentiality where a tender respondent's intellectual property/commercial information is not protected, resulting in IoT service provider complaints,	• Establish formal security procedures to ensure tenders are handled securely: ○ Use eTendering to manage receipt of tenders and secure systems to store information ○ Restrict access to tenders to the evaluation committee and/or make staff with access to

Procurement risk	How to avoid it
mistrust or political intervention	tenders sign a code of conduct and declaration of conflicts of interest ○ Check conflict of interests arising during evaluation at the start of each meeting ○ Keep thorough records, record any conflicts and mitigation actions. • Perform regular security audits and reviews, advise IoT service providers of security measures, and train staff.
Organisation does not own IoT data collected and the IoT service provider limits or prevents the organisation from accessing the data	• The procurement specifications and the contract need to explicitly state who owns the raw data. It is recommended that your organisation owns the raw data to give you flexibility to use the raw data other purposes (e.g. data analysis and combining with different data sets).
Selection of inappropriate goods/services means the IoT service provider's solution does not meet the desired outcome	• Involve end users in the evaluation • Make sure the evaluation panel has or can access the relevant technical expertise. Refer to the UN Procurement Practitioner's Handbook for more information.

5.1.8 Disposal of assets

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

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

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

5.2 Data considerations for contracting

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

5.2.1 Data handling

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

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

5.2.2 Data ownership and rights

a) Data ownership and control

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

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

Case Study – Intellectual property and data access

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

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

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

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

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

b) Exclusive rights to use of data

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

Where fair to affected individuals and reasonably practicable, data about public activities of citizens that government agencies cause or facilitate to be generated should be treated as a public asset and made available as open data as widely as possible.

c) New datasets

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

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

d) Data retention and destruction obligations

All government data held by an IoT service or service provider should be contractually required to be returned to government (in a format specified by government) at the end of a contract, or when a service or relationship with an IoT service provider is discontinued.

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

5.2.3 Data quality requirements

a) Data quality issues

Data quality issues caused by device breakdowns or device calibration can generate incorrect or inaccurate data which can lead to incorrect decision making. If this poses unacceptable business or customer risk, use your contract to define data governance requirements and required mitigations that minimise the likelihood of these risks. This can include:

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

b) Liability arising from data quality

You need to be transparent about any potential quality issues in license or sharing agreements if the data will be made available to others as open data or as shared data. Depending on the strength and resilience of your IoT network, it may be important to flag in any contracts or sharing agreements that data may be incomplete, intermittently available or otherwise unreliable if there are connectivity or outage issues impacting your IoT network. This will help protect against any liability claims.

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

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

5.2.4 Data privacy and security

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

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

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

5.2.5 Application Programming Interfaces (APIs)

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

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

5.2.6 Cloud storage

NSW Government has evaluated and endorsed a panel of cloud service providers that are available to agencies to contract via buy.nsw (use of buy.nsw is not mandatory). In contract arrangements with cloud providers, you need to ensure that:

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

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

5.2.7 Establishing clear responsibilities

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

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

5.3 Key contract terms for IoT solutions

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

Contract term	What needs to be covered in the contract?
Data	See the Chapter 5.2 Data considerations for contracting.
Privacy	• Any relevant privacy provisions. For example, the IoT service provider may be required to have and maintain a privacy policy, data security policy and/or audit requirements to ensure the service provider's compliance in relation to the principal's data held by the service provider.
Intellectual property	• Specify who owns the intellectual property. The NSW Government default position is that the service provider owns the intellectual property and must grant a perpetual, transferable, royalty free licence for the NSW Government agency to use it.
Transfer/right of use by other agencies	• The contract should consider the need to transfer contracts, products or licences to other organisations in future (for example, due to Machinery of Government changes).
Multi-agency access contracts "Piggybacking" clauses	• Piggybacking is where one organisation has established an arrangement and has made the arrangement available to other organisations. Piggybacking requires organisation to accept the terms and conditions of the existing contract. • You need to consider if it is appropriate to permit other organisations to use the contract. Guidelines on inclusion of piggyback clauses and sample clauses to be incorporated into market documents can be found at ProcurePoint. • At a minimum ensure the contract does not include a confidentiality requirement that prevents the contract being provided to other organisations.
Supply chain integrity	• An IoT service provider must maintain the integrity and security of its supply chain. This includes contractual undertakings for the IoT service provider to provide the client with information about its local and global supply chain as it relates to, or impacts on, the hardware and software provided as part of an IoT network. For more information on supply chain risk, see the Cyber security chapter.
IoT service provider conduct	• IoT service providers must meet minimum standards of conduct in ethical behaviour. If they breach the expected level of behaviour (corruption, fraud, breach of govt policy, etc.), you need to reserve the right to take action, up to and including termination of the contract.