Managing Cyber Security in Procurement Guideline

Managing Cyber Security in Procurement Guideline

Version Control

#	Date	Changes
1.0	June 2025	
1.1	May 2026	Updated branding, minor updates to correct broken links and inclusion of Foreign ownership, control, or influence (FOCI) information

Contact us

Engage with your agency's cyber security team as first point of contact, which is usually located within the division responsible for the agency's information and communication technology (ICT). Further support can be requested from the Queensland Government Cyber Security Unit (CSU) via cybersecurityunit@qld.gov.au, or visit www.qld.gov.au/cybersecurity.

Disclaimer

This document is intended as a guide only for the internal use and benefit of government agencies. It may not be relied on by any other party. It should be read in conjunction with the Queensland Procurement Policy, Information and cyber security policy (IS18), your agency's procurement policies and procedures, and any other relevant documents.

The Department of Housing and Public Works disclaims all liability that may arise from the use of this document. This document should not be used as a substitute for obtaining appropriate probity and legal advice as may be required. In preparing this document, reasonable efforts have been made to use accurate and current information. It should be noted that information may have changed since the publication of this document. Where errors or inaccuracies are brought to the attention of the Department of Housing and Public Works, a reasonable effort will be made to correct them.

Table of Contents

1. Introduction

1.1 Purpose

With the growing number of suppliers to Queensland Government and the increasing digital connectivity of these businesses, this guideline was created to support the management of cyber security risks across all types of procurement.

This guideline aims to complement Procurement and Cyber Security practices to enable agencies to effectively manage risk by leveraging cyber security controls. By leveraging the security criteria in this guideline, Queensland Government is safeguarding the delivery of important goods and services to Queensland and the businesses within the supply chain. Incremental capability improvements across supply chains will lead to strengthened collective resilience to cyber security incidents (***Appendix B***).

This guideline applies to the purchase of **all goods**, **products, and services** – and is not limited to information, communication, and technology (ICT) procurement.

It is recommended that this guideline is leveraged as part of contract management with existing suppliers so they can strengthen their security posture and that of the supply chain. Suppliers to Government, including their suppliers (i.e. the supply chain), should proactively apply these controls to improve their security posture.

1.2 Audience

This document is primarily intended for Queensland Government agency staff responsible for, leading, or supporting the procurement of goods, products, and services.

This guideline applies to all Queensland Government agencies and entities.

Agency staff should consult with stakeholders within their agency to support the application of this guideline. Key stakeholders may include:

Stakeholder	Involvement
Business subject matter experts (BSME)	Initiates a procurement process to acquire goods and services, with an understanding of the workplace's specific needs, including potential information exposure and proposed expenditure.
Service Owner	Responsible for the product or service that is being procured from the market. Should be involved in making key decisions and approvals.
Procurement officers (PO)	Collaborate with BSMEs to provide guidance on the documented procurement process and address business needs, including assisting with the completion of a value risk matrix (VRM).
Cyber security expert (CSE)	Has expertise and can offer support regarding cyber security risks and information security, along with their effects on procurement processes.
Privacy impact officer (PIO)	Understands the organisation’s privacy obligations and their impact on procurement processes, assisting in completing a Privacy Impact Assessment (PIA).
Risk officers (RO)	Collaborate with BSMEs to identify and assess risks, developing preventive measures to avoid, reduce, or transfer them. Also assist in completing a risk register.
Suppliers	Engaged through the procurement process (i.e. through a request for quote (RFQ) or other mechanism), communicates with the BSME and/or purchase order (PO) about their goods/services and security posture, any supply chain impacts, and third-party suppliers (which may include sub-contractors).

1.3 Scope

This guideline relates to the application of the Queensland Procurement Policy and the requirements of the Information and cyber security policy (IS18).

This guideline provides recommendations on using principles and controls to support mitigating risk but does not recommend or include specific contract clauses. The security criteria within this guideline are intended as suggestions only. Additionally, this guideline does not cover specific control implementation or detail activities that follow this stage (e.g. contract management).

Agencies are encouraged to review this guideline, including the additional resources contained within, and develop supporting material (e.g. processes and procedures). These materials should cover roles and responsibilities, specific tasks/activities, and links to related materials/tools (e.g. agency risk management, information asset register). It is also recommended that agencies develop and facilitate training to maximise awareness and competence in managing cyber security in procurement and the supply chain.

2. Guideline Overview

This guideline consists of three key stages:

Stage 1 - Identify: Identify and define the goods and/or services being procured and the information that will be shared with, used, acquired or created by the supplier.

Stage 2 - Assess: Assess agency risk, procurement value/risk, and information security. Determine what impact/risk threshold has been reached. Existing tools such as the Value/Risk Assessment and Information Security Classification Assessment are used to streamline this process.

Stage 3 - Apply: Provides recommended security criteria for agencies to leverage during procurement process, offering guidance on when and what to consider ensuring suppliers apply and meet these security criteria.

A set of Essential Security Criteria is defined in this guideline and is recommended as a minimum benchmark for purchasing from suppliers.

Engaging with key stakeholders within the agency for support throughout the three stages contained in this guideline is crucial. Key stakeholders should not be limited to the audience defined in this guideline.

For additional guidance on how to practically apply this guideline, examples have been created and can be viewed in ***Appendix C***.

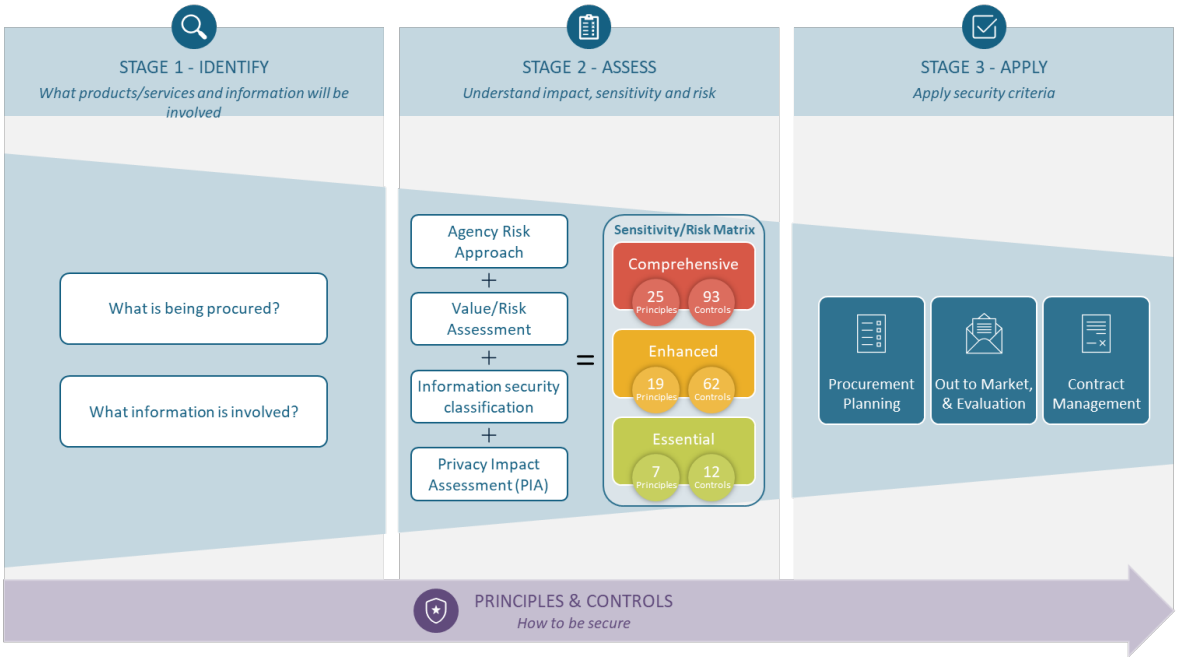


Figure 1 – Guideline Overview

3. Stage 1 - Identify

The purpose of this stage is to understand what information that will be shared with, used, acquired or created by a supplier as part of a future contract with the Queensland Government when products and/or services are being provided.

`3.1 What is being purchased?

An agency should clearly define the product or service that is being sought from the market. This will form the foundation for risk management throughout the procurement process. Agencies should consider the following:

- Is the product or service clearly defined?
- Who will be the owner of the product or service?
- Is it a once off purchase of a common-use supply arrangement?
- Are there any existing products or services that depend on or are connected to this new product or service?
- Where does this product or service fit into the supply chain (i.e. does it involve other customers/agencies, suppliers and/or the public)?
- Who is receiving the product or service (i.e. the agency, the agency's employees, or the public)?

3.2 What information is involved?

Once the product and/or service to be purchased is identified, it is critical to determine the information needed for the supplier to deliver it effectively.

An agency should identify what information may be shared with, used, acquired or created by the supplier. An agency should consider the following:

- What information will the supplier have access to (e.g. employee names, office addresses, project information, business plans, etc)?
- Is any personally identifiable information likely to be involved (agencies can undertake a Threshold Privacy Assessment to help determine this)?
- Will information be shared once?
- Will the supplier have access to information over a prolonged period (i.e. purchasing a service delivered over multiple years)?
- Where will information be shared (e.g. O365 environment, stored or hosted by the supplier, emails, print outs, etc)?
- Will the agency retain control of the platform where information is shared (i.e. is it being shared via a SharePoint site managed by the agency or the supplier)?

An effective method of identifying information that may be exposed to the supplier is using the agency's information asset register. Through cataloguing information as an information asset, an agency can support more considered steps to mitigate cyber risk (such as those listed in (***Appendix B***).

3.2.1 Leveraging an agency's information asset register

The Information Asset Custodianship Policy (IS44) requires agencies to identify their holdings of information assets and establish an information asset register. Often, information asset registers will also have the information security classification, which relates to an assessment that is completed in Stage 2 of this guideline (*4.3 Information Security Classification* Assessment).

Information may include: customer data (names, addresses), financial data (budgets, bank account details, credit card numbers), corporate data (business plans), human resource data (employee details and records), and technical data (software/system configuration).

Information Asset Register							
#	ID	Name	Type	Owner	Custodian	Classification	Location
1	Asset-01	Customer Data	Database	Chantel	Customer Service	Sensitive	Digital (SAP)
2	Asset-02	Employee Data	Database	Fiona	Human Resources	Protected	Digital (SAP)
3	Asset-03	Strategy Plan	Document	Glenn	Strategy Team	Official	Digital (Sharepoint)
4	Asset-04	Project Plan	Document	Ash	Project Management Team	Official	Physical (Paper)
5	Asset-05	Financial Statements	Software	Nathan	Finance Team	Official	Digital (Excel)

Figure 2 – Example Information Asset Register

More information can be found in the Information asset register guideline | For government | Queensland Government.

3.3 Risks associated with foreign owned, controlled or influenced suppliers

Foreign owned, controlled or influenced (FOCI) risks in the supply chain refer to the ability for suppliers to be directed by a foreign government to conduct malicious activities. This can be through direct business ownership channels, the domestic laws of a foreign jurisdiction, or other sources of outside influence:

- **Foreign ownership:** The degree to which foreign countries possess ownership stakes in a company, its subsidiaries, and its affiliates. It could mean that a portion of the company's shares is held under foreign investment by a foreign person, foreign resident, or that a foreign company has significant equity interest. Foreign investments can also come through venture capital.
- **Foreign control:** The authority and influence exerted by foreign entities and governments over a company's decision-making processes. This can involve legislation allowing the use and access of data and communications generated and stored by industry in a foreign country, the appointment of key personnel, board members, or other measures that grant foreign interests a say in how the company operates.
- **Foreign (malign) influence:** Can be applied on suppliers through various coercive means, including economic leverage, strategic partnerships, or even subtle political manoeuvring. When foreign actors or governments seek to exert influence in a way that is actively hidden or not transparent, this can have serious implications for organisations and Australia.

Having identified what information may be shared with, used, acquired or created by the supplier, an agency should consider identifying the need for a more rigorous examination of FOCI risks, then include FOCI risk analysis as part of the next Stage.

4. Stage 2 - Assess

The purpose of this stage is to evaluate risk and impacts relating to the product or service and information involved. This stage steps through the agency's risk approach, procurement value/risk matrix, information security classification, and brings it all together by determining the overall impact/risk threshold reached. It's important to consistently engage internal key stakeholders for support through assessments contained in this section.

4.1 Agency Risk Approach

An agency's risk appetite and management approach should be considered throughout the application of this guideline. General considerations relating to risk management should be made:

- What is the general risk appetite of the agency (e.g. low, medium, high)?

- How critical is the product or service to the agency?
- How critical is the service to Queensland and the community?
- Are there defined risk tolerance levels that should be applied?
- How will the risk change dependent on the length of engagement?

4.2 Value/Risk Assessment

As a part of the procurement process, the Value/Risk Matrix (VRM) should be used to assess the associated value and risk. This simple tool asks eleven multi-choice questions that will result in the procurement being categorised as – Routine, Leveraged, Focused, or Strategic.

When addressing these questions, focus particularly on those related to operational impact, product/service availability, and the supply market. Record the result of this assessment.

Value Risk Matrix (VRM) for sourcing goods or services		Updated November2019	
This VRM can be used to assess the complexity (based on value and risk) of a sourcing activity for goods or services.			
What goods/services are you sourcing (buying)?			
Question	**Answer**	**Score**	**Comments**
Risk Questions (X axis)		**46**	
Q1. Do the specifications of the goods/services require customisation?	Yes, however the goods/services only require a low level of customisation (e.g. small/minor configuration or specialisation)	4	
Q2. Are the goods/services critical to the organisation and/or its core operations?	Yes, the goods/services are highly critical (i.e. fundamental) to the organisation and/or core operations (e.g. direct impact on critical front line services)	9	
Q3. Are the goods/services being purchased from a competitive market? Competitive market includes consideration of substitute goods/services and the suppliers within that market	No, only one suitable substitute or supplier has been identified and qualified (e.g. where prior intellectual property has been co-developed with a	9	
Q4. Will the purchase(s) impact the market?	Yes, the procurement is likely to result in the creation of a monopoly or potential market power by government	6	
Q5. Would there be a significant interruption to the organisation's core operations if the supplier defaults?	Yes, there would be a significant interruption (major or severe risk) to the organisation's core operations with a high transition time to an alternate supplier	12	
Q6. Are there local industry considerations with this purchase? E.g. recognise the impact of international suppliers on participation by local businesses.	Yes, changes to the level of international market participation will impact local suppliers	6	
Q7. What level of confidence do stakeholders and/or the community (if relevant) have that the required outcome(s) will be delivered?	High: The community and/or stakeholders have a high level of confidence that the required outcome(s) will be delivered	0	

Figure 3 – Value/Risk Matrix (risk questions [completed example])

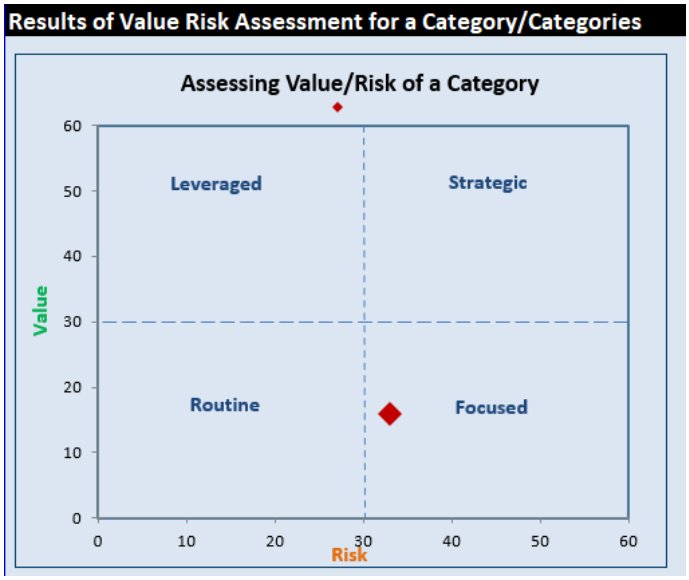


Figure 4 – Value/Risk Assessment outcome (Focused)

4.3 Information Security Classification Assessment (Business Impact Levels)

An agency should conduct an information security classification assessment on each of the involved information assets as per the Information security classification framework (QGISCF). This framework assesses the business impact levels (BILs) and will result in the information/data being categorised as Low, Medium or High for each of the three BILs which relate to Confidentiality, Integrity and Availability (CIA).

Record the highest BIL result across all three categories (i.e. Low Confidentiality, High Integrity, Low Availability – the result is 'High').

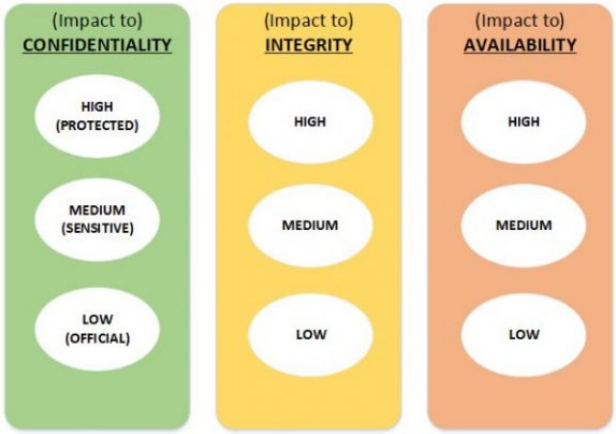


Figure 5 – Information Security Classification Framework

4.4 Personally Identifiable Information

Where agencies have identified that the product and/or service will involve personally identifiable information (PII) (e.g. through a Threshold Privacy Assessment), then it is highly recommended that a Privacy Impact Assessment is conducted by the agency.

Agencies should consult their agency's procedures (or where none is available the step-by-step guide to Privacy Impact Assessments) for guidance on managing (PII), as this guideline does not cover this topic.

4.5 Which Impact/Risk Threshold has been Reached?

Use the results from the 4.2 Value/Risk Assessment and the 4.3 Information Security Classification Assessment to determine which Threshold (Essential, Enhanced, or Comprehensive) has been reached on the Impact/Risk Matrix (Figure 6) below.

These Thresholds are intended to offer an indicative framework for managing cyber security during the procurement lifecycle by providing a set of security criteria for agency's use.

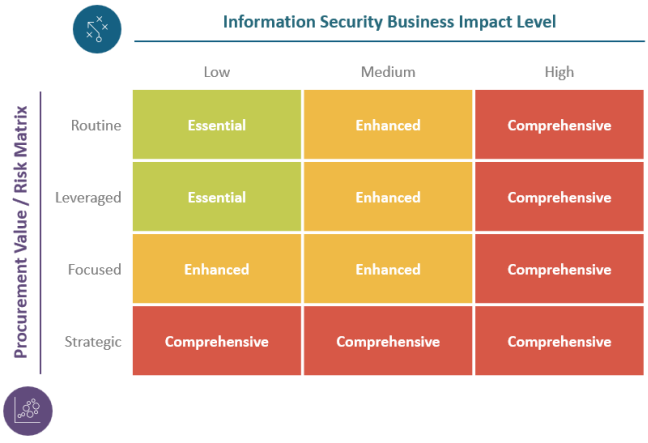


Figure 6 – Impact/Risk Matrix

4.6 Potential for FOCI risk?

At this stage an agency will have a good understanding of the criticality of the product or the service and will have identified whether FOCI risks require additional attention in the planning stage of the procurement.

If FOCI considerations are identified as relevant to the procurement activity, refer to the flowchart (Figure 7) from the Department of Home Affairs' Foreign Ownership, Control or Influence Risk Assessment Guidance to determine if further dedicated analysis of FOCI risks is required.

Application of this Guidance should be undertaken within the context of the organisation's risk management arrangements.

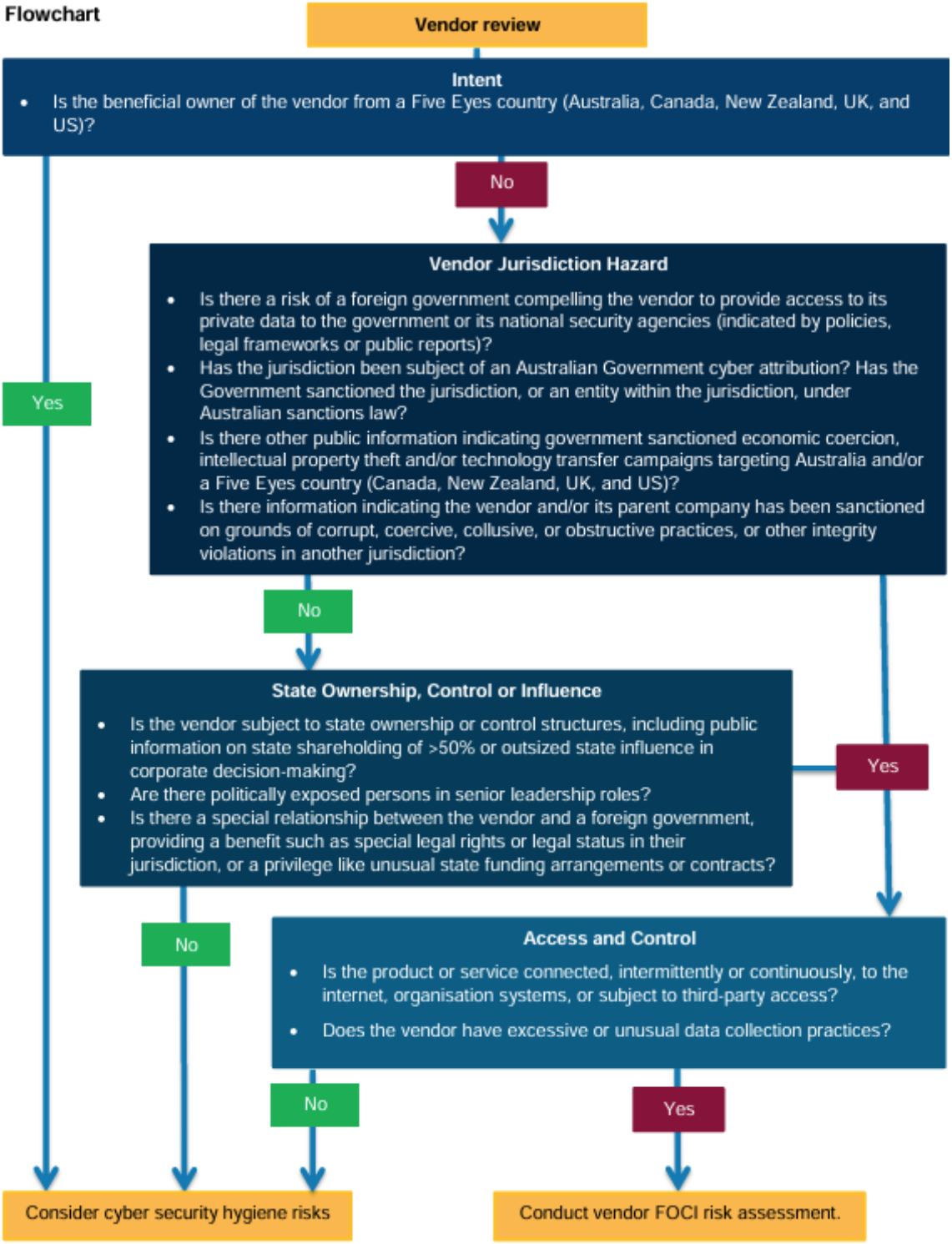


Figure 7 – FOCI risk consideration flowchart. Source: Commonwealth of Australia, Department of Home Affairs, *Foreign Ownership, Control or Influence Risk Assessment Guidance, 2026*.

5. Stage 3 - Apply

This stage defines and specifies the Security Criteria (Principles and Controls), details considerations to take into account before applying these criteria, and provides guidance on their usage throughout the procurement process. It is important to note that the Principles and Controls are not directly related and should be reviewed separately.

5.1 Threshold Security Criteria

The established Security Criteria for each Threshold includes a set of Principles and Controls that suppliers should meet when conducting business with the Queensland Government. As each Threshold is reached, all lower-level Principles and Controls should be applied alongside the security criteria of that specific Threshold (see Figure 7). It is important to recognise that these criteria are a guide, and agencies are encouraged to review them holistically to ensure they meet the specific needs of the agency and the procurement process. Principles and Controls are listed in the next section of this document.

Figure 7 – Threshold Security Criteria

Essential Security Criteria have been developed to support the maturity growth of organisations throughout Queensland. These criteria have been designed so that businesses can achieve it without a large investment of time or resources. It aims to provide Queensland Government supply chains with a basic level of protection and response capability. The Essential criteria should be considered as a minimum irrespective of what product or service is being purchased.

Enhanced Security Criteria adopts a stronger approach by supplementing the Essential controls with an additional layer of security. To support the application of this Threshold, it is recommended to engage the agency's Cyber Security specialists.

Comprehensive Security Criteria is an extensive set of cyber security controls that should be considered during the procurement of goods or services with higher information sensitivity or risk averse approaches. To support the application of this Threshold, it is highly recommended to engage the agency's Cyber Security specialists.

5.2 Principles and Controls

This section defines and lists the Principles and Controls that agency staff should utilise. Agencies should review this section, noting any Principles and Controls that correspond with the reached Threshold and any additional Principles and/or Controls that address their agency's specific needs and risk management.

It is important to remember that these Principles and Controls are intended for the supplier to meet, not the agency.

5.2.1 Principles and Controls

The Australian Signals Directorate Information Security Manual defines Cyber Security Principles which provide strategic guidance on how an organisation can protect themselves from cyber threats. These Principles are grouped into five functions: Govern, Identify, Protect, Detect, Respond.

All Principles should be reviewed and considered throughout the procurement process, with particular attention to how they might mitigate specific risks. To support practical application, the Principles have been aligned with each Threshold in the Impact/Risk Matrix (as detailed in section 4.5).

Functions	Details	Essential	Enhanced	Comprehensive
GOVERN Develop a strong cyber security culture	A Chief Information Security Officer provides leadership and oversight of cyber security.			●
	Security risk management activities for systems, applications and data are embedded into organisational risk management frameworks.		●	●
	Security risks for systems, applications and data are accepted before they are authorised for use and continuously throughout their operational life.			●
IDENTIFY Identify assets and associated security risks	The business criticality of systems, applications and data is determined and documented.		●	●
	The confidentiality, integrity and availability requirements for systems, applications and data are determined and documented.		●	●
	Security risks for systems, applications and data are identified and documented.		●	●
PROTECT Implement controls to manage security risks	Systems and applications are designed, deployed, maintained and decommissioned according to their business criticality and their confidentiality, integrity and availability requirements.		●	●
	Systems and applications are delivered and supported by trusted suppliers.	●	●	●
	Systems and applications are designed and configured to reduce their attack surface.			●
	Systems, applications and data are administered in a secure and accountable manner.		●	●
	Vulnerabilities in systems and applications are identified and mitigated in a timely manner.		●	●
	Only trusted and supported operating systems, applications and code can execute on systems.		●	●
	Data is encrypted at rest and in transit between different systems.		●	●

Functions	Details	Essential	Enhanced	Comprehensive
	Data communicated between different systems is controlled and inspectable			●
	Applications, settings and data are backed up in a secure and proven manner on a regular basis.		●	●
	Only trusted and vetted personnel are granted access to systems, applications and data.		●	●
	Personnel are granted the minimum access to systems, applications and data required to undertake their duties.	●	●	●
	Robust and secure identity and access management is used to control access to systems, applications and data.	●	●	●
	Personnel are provided with ongoing cyber security awareness training			●
	Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel.	●	●	●
DETECT Detect and analyse cyber security events to identify cyber security incidents	Event logs are collected and analysed in a timely manner to detect cyber security events.			●
	Cyber security events are analysed in a timely manner to identify cyber security incidents.		●	●
RESPOND Respond to and recover from cyber security incidents	Cyber security incidents are reported internally and externally to relevant bodies and stakeholders in a timely manner.	●	●	●
	Cyber security incidents are analysed, contained, eradicated and recovered from in a timely manner.	●	●	●
	Incident response, business continuity and disaster recovery plans support the recovery of normal business operations during and following cyber security incidents.	●	●	●

5.2.2 Controls

A control is a measure that maintains and/or modifies risk. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Derived from best practice Cyber Security Frameworks, the Controls in this guideline are grouped into four categories: Organisational, People, Physical, Technological.

All Controls should be reviewed and considered throughout the procurement process, with particular attention to how they might mitigate specific risks. To support practical application, the Controls have been aligned with each Threshold in the Impact/Risk Matrix (as detailed in section 4.5). Controls can be found in ***Appendix A***.

The description of the control categories is outlined below:

Organisational	Policies, processes, and structures that support cyber security management.
People	Roles, responsibilities, and skills of the staff and stakeholders involved in cyber security.
Physical	Protection of the physical assets and environments that store or process information.
Technological	Selection, implementation, and maintenance of the technical measures that safeguard information.

5.3 Determining expectations of suppliers

With the Principles and Controls now identified, agencies should consider how suppliers are expected to meet these requirements before, during, and after product/service delivery with the Queensland Government. Given that each agency's approach to procurement may vary, it is crucial to apply the Principles and Controls in accordance with the specific needs of the agency and each procurement process.

Here are some questions to help guide the conversation:

- Have we engaged with this supplier in the past?
- What is the maturity of the supplier?
- Is evidence required (once off or annually) or is general acknowledgement sufficient?
- Is the control required on the whole supplier's business or just specific components?
- What certification meets the agency's suitability requirements/benchmark (e.g. ISO/IEC certification, SOC 2, PCI DSS)?
- Does the supplier need to have been independently cyber assessed?
- Should the control extend to the supplier's suppliers (3rd & 4th party suppliers)?
- How long should the requirement be set for, in line with the contract term or for a longer period?
- How does the agency interpret the Principle/Control (i.e. what does 'trusted suppliers' mean to our agency)?
- What would trigger a review of identified security criteria (i.e. change to threat environment)?

5. 4 When to apply

Principles and Controls should be considered throughout the entire lifecycle of a procurement process, but specifically at the time of engaging a supplier.

The utilisation of the security criteria will vary during each stage of the procurement lifecycle (i.e. one control may be appropriate to add into the requirements specification ['Access control'], whereas another control may be appropriate when offboarding a supplier ['Information deletion']).

Below are some examples of when the criteria may be relevant:

Stage	Examples of when security criteria may be relevant
Planning	- Developing procurement plans and identifying scope, complexity, opportunities and risks - Conducting market analysis - Identifying tender strategy and method - i.e. via a common-use supply arrangement, open or limited tender - Identifying stakeholders - Identifying what information/data will be shared with, used, acquired or created by the successful supplier/s

Out to Market and Evaluation	- Defining the requirements / specifications
	- Determining criteria - mandatory vs desirable criteria
	- Determining insurance requirements and the minimum values
	- Determining appropriate systems and security questions, including how they will be assessed for risks - not limited to:
	  ○ who is hosting the information/data
	  ○ where the information/data is located
	  ○ security posture and
	  ○ business continuity plans/learnings
	- Developing appropriate clauses to support implementation (transition in), on-going management and termination (transition out)
	- Supplier negotiations

Contract Management	- Transitioning/implementing supplier/s - Developing a contract management plan - Periodically reviewing the supplier's security profile and if there are any changes to the information/data shared with, used, acquired or created by the supplier - Conducting periodic audits and compliance checks - Developing incident response plans (which may be conducted in partnership with supplier/s) - Reviewing/updating contractual controls, where the supplier's security profile changes - Transitioning out suppliers – including offboarding, identifying survival clauses and secure return/disposal of data

6. Additional resources

The following additional resources may support the implementation of this guideline:

Description	Resource
Australian Government Guidance	Identifying Cyber Supply Chain Risks | Cyber.gov.au
	Essential Eight | Cyber.gov.au
	Information Security Manual (ISM) | Cyber.gov.au
	Factsheet Security standards for smart devices
	Foreign Ownership, Control or Influence Risk Assessment Guidance
Queensland Government Standards and Practices	Data encryption standard | For government | Queensland Government
	Procurement guidance | For government | Queensland Government

Description	Resource
	Cyber security obligations and better practice | For government | Queensland Government
Queensland Government Frameworks	Queensland Government authentication framework (QGAF) | For government | Queensland Government
	Queensland Government contract management framework | For government | Queensland Government
	Queensland Government information security classification framework (QGISCF)
Queensland Government Information Standards, Practices, and Guides	Information asset custodianship policy (IS44)
	Information Sharing Authorising Framework
	Information Management Principles
International Standards and Practices	Good Practices for Supply Chain Cybersecurity — ENISA (europa.eu)
	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (nist.gov)
	ISO/IEC 27036-1:2021 - Cybersecurity — Supplier relationships — Part 1: Overview and concepts
Queensland Government Definition Glossary	Glossary

6.1 Need more help?

Engage with your agency's Cyber Security team as first point of contact, which is usually located within the division responsible for the agency's information and communication technology (ICT).

Further support can be requested from the Queensland Government Cyber Security Unit via cybersecurityunit@qld.gov.au, or visit www.qld.gov.au/cybersecurity.

Appendix A Security Criteria (Controls)

As per section 5.2 Controls, this table lists cyber security controls for an agency to leverage during the procurement process.

Category	Control	Details	Essential	Enhanced	Comprehensive
Organisational	Policies for information security	The supplier has a clear information security policy that is approved, shared with staff, and reviewed regularly.		●	●
	Information security roles and responsibilities	The supplier clearly defines and assigns information security roles based on their needs.			●
	Segregation of duties	The supplier separates conflicting tasks and responsibilities.			●
	Management responsibilities	The supplier ensures all staff follow established information security policies and procedures.		●	●
	Contact with authorities	The supplier maintains communication with relevant authorities regarding information security issues.		●	●
	Contact with special interest groups	The supplier engages with professional groups and security forums for support and best practices.			●
	Threat intelligence	The supplier gathers and analyses data relating to potential information security threats.			●
	Information security in project management	The supplier integrates information security practices into their project management processes.			●
	Inventory of information and assets	The supplier keeps an updated list of all information and assets, including their owners.		●	●
	Acceptable use of information and assets	The supplier has documented rules for acceptable use of information and assets.		●	●
	Return of assets	The supplier ensures all organizational assets are returned when personnel leave or change roles.	●	●	●
	Classification of information	The supplier classifies information based on its confidentiality, integrity, and availability.		●	●
	Labelling of information	The supplier follows procedures for labelling information according to its classification.			●
	Information transfer	The supplier has established rules and agreements for transferring information.	●	●	●
	Access control	The supplier implements rules for who can access information and assets.	●	●	●
	Identity management	The supplier manages user identities throughout their lifecycle.			●

Category	Control	Details	Essential	Enhanced	Comprehensive
	Authentication information	The supplier controls the assignment and management of authentication details.		●	●
	Access rights	The supplier provisions, reviews, and modifies access rights according to policies.	●	●	●
	Information security in supplier relationships	The supplier has processes to manage information security risks related to their products or services.			●
	Addressing information security in supplier agreements	The supplier addresses and manages information security requirements in contracts with their suppliers.			●
	Managing information security in the supply chain	The supplier has procedures to manage information security risks in their supply chain.			●
	Monitoring supplier services	The supplier regularly reviews and manages their information security practices.			●
	Information security for cloud services	The supplier has rules for acquiring and using cloud services securely.			●
	Incident management planning	The supplier has defined roles and processes for managing information security incidents.	●	●	●
	Assessment of security events	The supplier evaluates information security events to determine if they are incidents needing action.	●	●	●
	Response to incidents	The supplier follows documented procedures to respond to information security incidents, including notifying organisations within their supply chain.	●	●	●
	Learning from incidents	The supplier uses lessons from incidents to improve their information security measures.		●	●
	Collection of evidence	The supplier has procedures for gathering and preserving evidence related to information security events.			●
	Information security during disruption	The supplier has plans to maintain information security during disruptions.			●
	Readiness for business continuity	The supplier ensures their systems are ready for continuity during disruptions.			●
	Legal and regulatory requirements	The supplier identifies and keeps updated on relevant laws and regulations affecting information security.		●	●
	Intellectual property rights	The supplier has measures in place to protect intellectual property rights.		●	●
	Protection of records	The supplier protects records from loss, destruction, unauthorized access, and leaks.		●	●

Category	Control	Details	Essential	Enhanced	Comprehensive
	Privacy and personal information	The supplier complies with laws and regulations regarding privacy and protection of personal data.	●	●	●
	Independent review of security	The supplier undergoes independent reviews at planned intervals of their information security practices.			●
	Compliance with security policies	The supplier regularly checks that their staff follow information security policies and procedures.		●	●
	Documentation of procedures	The supplier documents operational procedures for information processing and makes them accessible as required.		●	●
People	Screening	The supplier conducts background checks on new hires and periodically thereafter.	●	●	●
	Terms and conditions of employment	The supplier includes information security responsibilities in employment contracts.		●	●
	Security awareness training	The supplier provides regular training on information security policies and procedures to their staff.		●	●
	Disciplinary process	The supplier has a clear process for addressing information security policy violations.		●	●
	Responsibilities after employment changes	The supplier communicates valid ongoing information security responsibilities after employees leave or change roles.		●	●
	Confidentiality agreements	The supplier requires employees and other interested parties to sign confidentiality agreements to protect sensitive information.		●	●
	Remote working	The supplier implements information security measures for employees working remotely.	●	●	●
	Event reporting	The supplier provides a mechanism for staff to report suspected security events.	●	●	●
Physical	Physical security perimeters	The supplier defines secure areas to protect information and assets.	●	●	●
	Physical entry controls	The supplier secures sensitive areas with appropriate access controls.	●	●	●
	Securing facilities	The supplier has physical security measures in place for their offices and facilities.	●	●	●
	Physical security monitoring	The supplier continuously monitors their premises for unauthorized access.		●	●
	Protection against threats	The supplier has protections against physical and environmental threats.		●	●
	Working in secure areas	The supplier implements security measures for work done in sensitive areas.		●	●

Category	Control	Details	Essential	Enhanced	Comprehensive
	Clear desk and screen policy	The supplier enforces rules for keeping desks clear of sensitive materials and locking screens.	●	●	●
	Equipment protection	The supplier ensures that all equipment is securely located and protected.		●	●
	Protection of off-site assets	The supplier safeguards assets stored off-site.		●	●
	Storage media management	The supplier manages the entire lifecycle of storage media, from acquisition to disposal.		●	●
	Supporting utilities protection	The supplier protects their systems from power outages and utility failures.		●	●
	Cabling security	The supplier protects power and data cables to prevent tampering or damage.		●	●
	Equipment maintenance	The supplier regularly maintains equipment to ensure information security.	●	●	●
	Secure disposal of equipment	The supplier ensures sensitive data is removed before disposing of or reusing equipment.		●	●
Technological	Protection of user devices	The supplier secures information on devices used by employees.		●	●
	Privileged access management	The supplier restricts and manages special access rights to sensitive systems.		●	●
	Access restrictions	The supplier restricts access to information based on established policies.		●	●
	Source code access	The supplier manages access to source code and development tools carefully.			●
	Secure authentication	The supplier uses strong authentication methods based on access policies (i.e. Multifactor authentication).	●	●	●
	Capacity management	The supplier monitors and adjusts resource usage based on current and future needs.		●	●
	Malware protection	The supplier implements measures to protect against malware and educates users about risks.	●	●	●
	Management of vulnerabilities	The supplier identifies and addresses technical vulnerabilities in their systems (i.e. patching).	●	●	●
	Configuration management	The supplier documents and manages the settings of hardware and software for security.		●	●
	Information deletion	The supplier deletes information when it is no longer needed.	●	●	●

Category	Control	Details	Essential	Enhanced	Comprehensive
	Data masking	The supplier uses data masking techniques to protect sensitive information.			●
	Data leakage prevention	The supplier applies measures to prevent unauthorized sharing of sensitive information.			●
	Information backup	The supplier regularly backs up important data and tests the backups.		●	●
	Redundant systems	The supplier has backup systems in place to ensure availability.			●
	Logging	The supplier produces logs of activities and events for review and analysis.		●	●
	Monitoring activities	The supplier continuously monitors for unusual activities that may indicate information security incidents.		●	●
	Clock synchronization	The supplier ensures that all systems use the same time source.			●
	Control of utility programs	The supplier limits and monitors the use of powerful utility programs.			●
	Software installation procedures	The supplier implements secure procedures for installing software on their systems.	●	●	●
	Network security	The supplier secures and manages networks to protect information.		●	●
	Security of network services	The supplier identifies and monitors security requirements for their network services.		●	●
	Network segregation	The supplier separates different information groups and services within their networks for added security.			●
	Web filtering	The supplier controls access to websites to minimize exposure to threats.		●	●
	Use of cryptography	The supplier defines and implements rules for using encryption securely.			●
	Secure development processes	The supplier establishes and applies rules for developing secure software and systems.			●
	Application security requirements	The supplier identifies and approves security needs during application development or acquisition.		●	●
	Secure system design	The supplier applies principles for secure system architecture during development.			●
	Secure coding practices	The supplier follows secure coding guidelines in software development.			●
	Security testing	The supplier conducts security testing throughout the software development process.			●

Category	Control	Details	Essential	Enhanced	Comprehensive
	Outsourced development management	The supplier monitors and reviews security practices in outsourced development.		●	●
	Separation of environments	The supplier keeps development, testing, and production environments separate and secure.			●
	Change management	The supplier manages changes to information systems and processes with proper procedures.		●	●
	Test information management	The supplier protects and manages information used for testing.			●
	Protection during audits	The supplier plans for secure audits and other assurance activities involving their operational systems.			●

Appendix B List of Cyber Security Incidents

Extracted from: Information security incident reporting standard.

Term	Description
Abuse of privileges	Unauthorised changes to privileged user settings on stand-alone or networked equipment including network profiles, local user or device configuration files that have not been approved through the Departments change management process.
Account Compromise	The compromise of Queensland Government account credentials providing unauthorised access to a malicious 3rd party. This often involves leveraging the targets position of trust, or escalating privileges to move laterally. Types of account compromises include: • Business email compromise • Local credentials (LAN) • Administrator credentials • SaaS Credentials.
Intrusions against networks	Intrusions targeting Queensland Government internal infrastructure. This includes but is not limited to: • Remote code execution • Denial-of-service (DoS)/distributed denial-of-service (DDoS) • Website defacements • Brute force attempts. Intrusions that cannot be attributed, after analysis, to what is considered consistent with Internet noise. For example intrusion attempts that consistently target internal network infrastructure, users or services provided for external use such as web applications.
Malware infections	Software programs designed to cause damage to Queensland Government systems.
Other events	Natural events and other events which result in damage to information and systems. This includes but is not limited to: • fire • flood • excessive heat • storms • biological agents • toxic dispersion • riots • power outage.
Password confidentiality	Sharing/stealing/loss of passwords or other authentication token.
Phishing	Emails or domains which masquerade as a legitimate entity with the goal of compromising a users information such as: • Access credentials • Personal information • Banking information.
Ransomware infections	Software programs designed to extort a payment, usually financial, by denying authorised user access to Queensland Government information systems.
Sabotage/physical damage	Any damage or destruction of physical information assets or electronic devices.
Suspicious system behaviour or failure (hardware/software) or communications)	Unknown network activities affecting/degrading network performance with increased network bandwidth usage and decreased response time, using excessive CPU, increased suspicious network requests or increased Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) alerts leading to application crashes.

Term	Description
Theft/loss of assets	The theft or loss of any information or technology asset/device (including portable and fixed media) that might have been or has been used to either process or store Queensland Government information.
Unauthorised access to information/systems	Unauthorised access from internal and external sources to Queensland Government information and systems.
Unauthorised changes to information, applications, systems or hardware	Any unauthorised changes to an organisations file system, including media, through insertion, modification or deletion. For example, changes to the standard operating environments (SOEs), addition of executables or the modification of an executables configuration. Any unauthorised installation of additional processing, communications or storage equipment into the IT network. This includes but is not limited to: • routers, switches, modems, firewalls • portable games units • USB devices • smart phones • wireless access points.
Unauthorised release of or disclosure of information	Unauthorised release or disclosure of Queensland Government information.
Violation of information security policy	Any violation of information security policy or the information security related aspects of the code of conduct.

Appendix C Applying this Guideline - Examples

Examples outlined in this section are fictitious and for **demonstration purposes only**. Agencies may choose to use these examples to support their own assessments and determine how to manage risk specific to the procurement activity.

Example #1: Professional Services

Background

I am a Queensland Government employee (business subject matter expert) tasked with engaging a supplier to provide professional services for human resources.

With the assistance of our agency's procurement officer, I have identified a suitable whole of Government common-use supply arrangement which I can use to buy these services and I have read the relevant guidance material on Queensland Government Arrangements Directory (QGAD).

Stage 1 - Identify

What is being purchased?

The supplier will be required to undertake research, conduct workshops/interviews, and develop a strategy relating to improving leadership skills of new and emerging managers, with this expected to be delivered within the next 6 months. I have written these requirements in the arrangement's Request for Quote (RFQ) template.

What information/data is involved?

Information will be gathered while the RFQ is out to market and once a Contract is awarded a supplier – of which this information will be publicly available.

The successful supplier will be provided with limited information (i.e. employee names, employee contact information, position titles and office address. No non-routine work information will be provided.

Stage 2 - Assess

Agency Risk Approach

This service would not be seen as critical and does not impact service delivery. It is a six-month project and limited information will be developed during this period. I engage the corporate risk team for support at this stage.

Value/Risk Assessment

With the help of the procurement officer, I've completed this assessment as part of my business as usual activities and assessed as ROUTINE.

Information Security Classification Assessment

Using our agency's information asset register I've determined the identified information/data has information security classification of OFFICIAL. I received 'low' results across confidentiality, integrity, and availability.

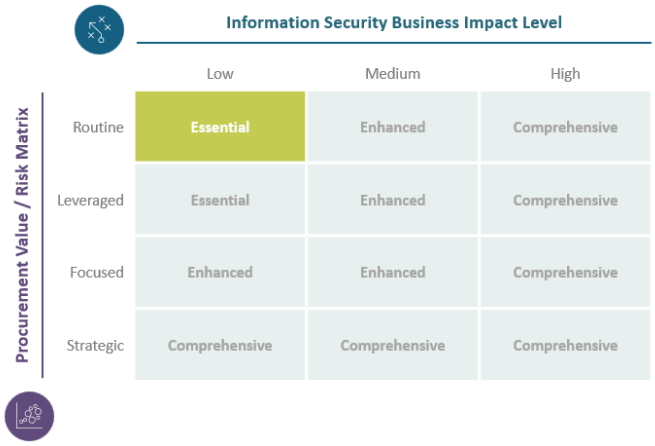
I also engage our cyber security team for support in validating the assessment results and for general support.

Privacy assessment

Working with the agency's privacy impact officer we completed the Threshold Privacy Assessment and determined that a privacy impact assessment was required. I provided all information required to inform the assessment report.

What Impact/Risk Threshold has been reached?

My assessments have identified my procurement activity as reaching the ‘Essential’ Threshold.



Stage 3 - Apply

Security Criteria

I have looked at the Essential security criteria and noted down the related principles and controls. After discussions with key stakeholders, we decided to also include some additional controls outside of the Essential threshold as these relate to the type of service I’m buying. These controls are:

- Policies for information security
- Legal and regulatory requirements
- Protection of records
- Security awareness training
- Disciplinary process
- Secure disposal of equipment
- Protection of user devices

Expectations of suppliers

I have interpreted the controls and am comfortable using them as-is and do not require evidence from the potential suppliers.

I will also make sure to check the supplier meets the controls when the engagement ends.

When to apply

I will be including the principles/controls as part of the governance / non-functional specification requirements to potential suppliers in my RFQ (by asking the suppliers to confirm they are able to comply).

My assessment of the suppliers’ response will assess any risks where suppliers are not able to confirm compliance and engage with stakeholders as appropriate to manage.

At the end of the contract (offboarding), I will ask for written confirmation that all relevant controls have been complied with (i.e. in line with “Secure disposal of equipment” control information relating to the engagement has been securely disposed of – whole of life approach to management of information).

Example #2: Police Car Tyres

Background

I am a Queensland Government procurement officer responsible for purchasing 1200 new tyres for police cars.

Stage 1 - Identify

What is being purchased?

I have been provided written specification requirements that will be used in the RFQ from the business subject matter expert (BSME). The successful supplier will provide tyres based on their ability to deliver upon the specified requirements.

What information/data is involved?

Information involved will be limited (i.e. delivery location, contract, invoicing and contact details).

Using our agency's information asset register I've determined corporate data will be exposed which has an information security classification of OFFICIAL. I also confirmed this classification with my Director

Stage 2 - Assess

Agency Risk Approach

This product is critical to front line service provision and police officer safety. It is a once-off purchase and limited information will be generated (e.g. purchase order, delivery locations, contract and invoicing details).

I take this opportunity to engage our corporate risk team to confirm my approach.

Value/Risk Assessment

I've already done this assessment as part of my BAU activities, and the output is 'Routine' due to the value of the contract.

Information Security Classification Assessment

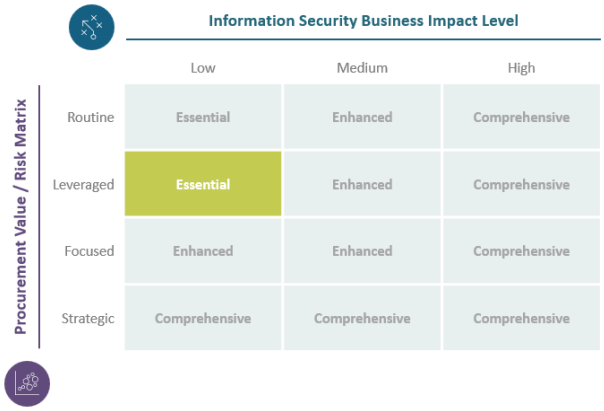
The information involved has classification of OFFICIAL and after conducting an assessment I received 'low' results across confidentiality, integrity, and availability.

Privacy assessment

I review the Threshold Privacy Assessment and engage the agency's privacy impact officer for support in understanding if I need to conduct any privacy related assessments. The privacy officer confirmed none are needed for this procurement process.

What Impact/Risk Threshold has been reached?

My assessments have identified my procurement as reaching the 'Essential' Threshold.



Stage 3 – Apply

Security Criteria

I have looked at the Essential security criteria and noted down the related principles and controls. Given that this is a once off purchase no additional controls will be used over and above the Essential security criteria.

How to apply

I have interpreted the controls and am comfortable using them as-is (as this is a one-time purchase) although my agency's risk appetite is low.

I am comfortable asking potential suppliers for confirmation (rather than evidence) of their ability to meet the principles and controls along with my other evaluation criteria and specification requirements. I am aware that there are standards that apply to the goods that I am purchasing.

When to apply

I will be including the principles/controls as part of my evaluation criteria in the RFQ, asking for written confirmation of compliance (but not proof at this stage). At time of offboarding I will ask for written confirmation that all relevant controls have been complied with (i.e. Information relating to the engagement has been securely disposed of).

Example #3: Employee Assistance Services

Background

I am a Queensland Government employee who needs to engage a supplier to provide employee assistance services for our department, our employees and their immediate family.

I have identified a suitable whole of Government common-use supply arrangement which I can use to buy these services and I have read the relevant guidance material on QGAD.

Stage 1 - Identify

What is being purchased?

A range of face to face and virtual (tele-health) services provided to employees and/or their immediate family throughout Queensland – with the services being provided from a range of health practitioners located throughout Australia.

What information/data is involved?

As part of the RFQ process, only routine work information will be provided - no personal or health information/data will be provided.

The successful supplier will be provided with, acquire or create a range of personal information (names, ages, gender, addresses, contact information), as well as personal health information.

Stage 2 - Assess

Agency Risk Approach

While this service would not be seen as critical and does not impact service delivery, supporting our employees (and their immediate family) mental health and wellbeing is critical, as well as during times of natural disasters

Value/Risk Assessment

I've completed this assessment and assessed as LEVERAGED.

Information Security Classification Assessment

Using our agency's information asset register I've determined the identified information/data has information security classification of SENSITIVE.

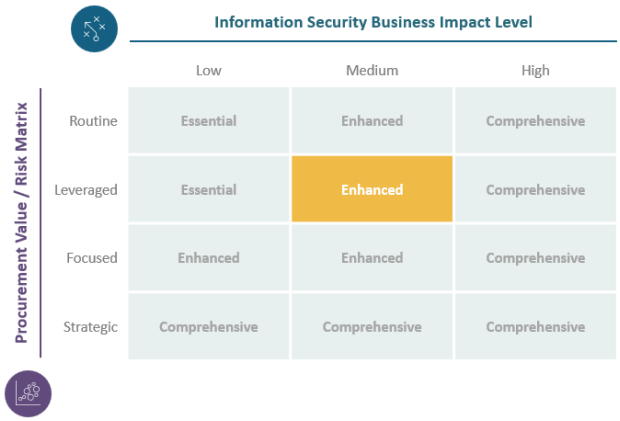
The information involved has classification of 'Sensitive' and after conducting an impact assessment, I received 'medium' results across confidentiality and 'low' results for integrity and availability, which results in a 'medium'.

Privacy assessment

Following a review of the Threshold Privacy Assessment, I determine and completed the privacy impact assessment with assistance from my agency's privacy impact officer.

What Impact/Risk Threshold has been reached?

My assessments have identified my procurement activity as reaching the 'Enhanced' Threshold.



Stage 3 - Apply

Security Criteria

I have filtered for the Essential security criteria from ***Appendix A*** and noted the related controls (refer to the below table).

Given that this is a once off purchase no additional controls will be used over and above the Essential security criteria.

In some cases, because of the way my department operates, some responsibilities will be managed internally (so it may be necessary to remove some of these from the supplier's responsibility).

Category	Control
Organisational	Policies for information security
	Management responsibilities
	Contact with authorities
	Inventory of information and assets
	Acceptable use of information and assets
	Return of assets
	Classification of information
	Information transfer

Category	Control
	Access control
	Authentication information
	Access rights
	Incident management planning
	Assessment of security events
	Response to incidents
	Learning from incidents
	Legal and regulatory requirements
	Intellectual property rights
	Protection of records
	Privacy and personal information
	Compliance with security policies
	Documentation of procedures
People	Screening
	Terms and conditions of employment
	Security awareness training
	Disciplinary process
	Responsibilities after employment changes
	Confidentiality agreements
	Remote working
	Event reporting
Physical	Physical security perimeters
	Physical entry controls
	Securing facilities
	Physical security monitoring
	Protection against threats
	Working in secure areas
	Clear desk and screen policy
	Equipment protection
	Protection of off-site assets
	Storage media management
	Supporting utilities protection
	Cabling security
	Equipment maintenance
	Secure disposal of equipment
Technological	Protection of user devices
	Privileged access management
	Access restrictions
	Secure authentication
	Capacity management
	Malware protection
	Management of vulnerabilities
	Configuration management
	Information deletion

Category	Control
	Information backup
	Logging
	Monitoring activities
	Software installation procedures
	Network security
	Security of network services
	Web filtering
	Application security requirements
	Outsourced development management
	Change management

In addition, I have also identified some Comprehensive threshold controls, which relate to the type of goods I am buying (refer to the below table).

Category	Control
Organisational	Policies for information security
	Legal and regulatory requirements
	Protection of records
People	Security awareness training
	Disciplinary process
Physical	Secure disposal of equipment
Technological	Protection of user devices
	Web filtering

Expectations of suppliers

Following advice from my agency's cyber security and procurement teams, we have developed a several mechanisms to seek evidence and compliance from potential suppliers as well as the successful supplier as part of ongoing contract management and contract end.

When to apply

I will apply these controls/principals throughout the procurement lifecycle:

Out to market	I will be including several principles/controls as part of the governance / non-functional specification requirements to potential suppliers in my RFQ (by asking the suppliers to confirm they are able to comply). I will be seeking information from suppliers as part of the Request for Quote (RFQ) to seek an understanding of the suppliers' ability to protect information/data (not limited to personal information and health records).
Evaluating offers	My assessment of the suppliers' response will assess any risks where suppliers are not able to confirm compliance and engage with key stakeholders as appropriate to manage. I will assess Suppliers' response to understand the supplier's capability, alignment with standards, best practices and any testing undertaken. I may seek advice from my agency's cyber security team to support this assessment.
Negotiation	I will develop specific clauses to support the protection of information/data in consultation with my agency's Legal and cyber security team and seek agreement from the preferred supplier and record them in the Contract. The clauses will place particular focus on

	ensuring the supplier maintains protection of employees' (and their immediate families) private and personal information.
Contract management	I will seek annual compliance certification from the supplier in accordance with the clauses developed with our cyber and legal teams.
Contract end	At the end of the contract (offboarding), I will ask for written confirmation that all relevant controls have been complied with (i.e. in line with "Secure disposal of equipment" control information relating to the engagement has been securely disposed of – whole of life approach to management of information).