Risk Management Guideline

Purpose

This Guideline provides practical advice about managing risk in the procurement of goods and services and in contract management.

Public authorities should refer to their internal risk management framework and supporting policies for guidance on risk criteria and how to analyse and assign levels of risk within the context of their public authority's risk profile.

Risk Management in Procurement

Risk management in procurement is about ensuring the risks associated with the purchase of goods or services are identified, assessed, managed and monitored to ensure unexpected or undesirable outcomes are minimised whilst achieving the objectives of the procurement, and identifying opportunities to improve performance.

Where procurement risk is well managed, project outcomes and objectives are more likely to be achieved.

When risk management processes are implemented, it ensures a proactive decision-making approach that seeks to avoid or minimise problems occurring. Systematically identifying what events might occur that will impact the procurement objectives, and the management of those risks, becomes integral to procurement as any other process. With effective processes in place, risks can be managed so that their impacts can be minimised or avoided altogether.

Ultimately, effective risk management in procurement supports the public authority in receiving the required goods or services on time and at the best possible quality, therefore ensuring business continuity, strong financial performance and value for all stakeholders (clients/end-users, suppliers, and the public authority).

South Australian Protective Security Framework

This guideline should be read in conjunction with the *South Australian Protective Security Framework* (SAPSF). Public Authorities are required to comply with the core and supporting requirements of SAPSF policy - *GOVSEC5: Managing the security of contractors and service providers*, which provides required actions and guidance related to security risks that can occur through the lifecycle of a procurement (including the contract management phase). GOVSEC5 contains recommended security terms and conditions for consideration.

Pursuant to the SAPSF, public authorities must:

1. *identify and mitigate security risks to the agency's people, information and assets generated by the procurement*
2. *ensure relevant security terms and conditions are included in contracts and service agreements that mange identified security risks to the procurement*

3. *manage and monitor:*
   a. *security risks for changes or incidents that could affect the procurement, service agreement or security of the agency*
   b. *the performance of the contractor (including subcontractors) over the lifetime of the contract*
4. *implement appropriate security arrangements to manage the completion or termination of a contract or agreement*

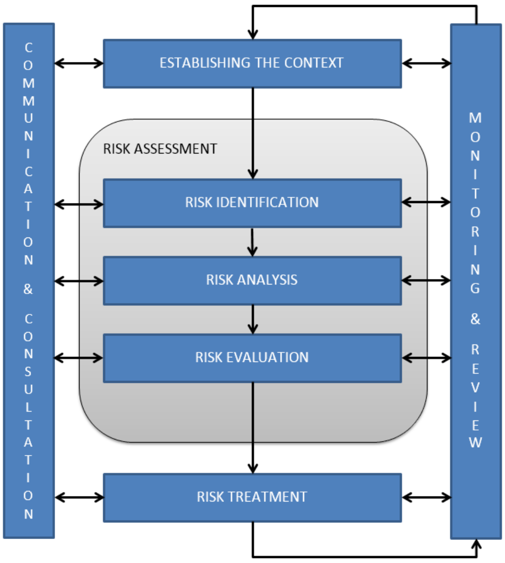
Risk Management Process

Public authorities should ensure that the effort directed to risk assessment and management is commensurate with the complexity of the procurement.

The risk management process identifies, and plans for, the potential risks that impact a project's procurement objectives. Planning for risk needs to occur at the earliest stages of planning for a procurement.

A risk management plan is often used to identify, analyse and document risk strategies associated with the procurement. More detail about the purpose of, and what to include in a risk management plan is outlined below under Step 6 of the Risk Management Process - *Developing a Risk Management Plan*.

The below figure[1] depicts the key elements (steps) of the risk management process and explains how each element (step) relates to procurement activities.



[1] based on AS/NZS ISO 31000:2009

Step 1: Establish the Procurement Context

The first step in establishing the procurement context is defining the key objectives to ensure there is a common understanding of what the procurement is aiming to achieve. Once the key objectives are defined, it is important to understand the environment in which the procurement is being undertaken and determine the contextual elements that are relevant to the procurement.

Issues to consider in establishing the risk management context include:

- legislation, standards and policies that are relevant to the procurement objectives (including, for example: SAPSF, Free Trade Agreements, etc.)
- external elements including the political, economic and competitive environment
- cross-agency, lead agency or individual agency responsibilities (as applicable)
- timeframes required to undertake the procurement activity
- stakeholders impacted by the procurement decision (including end-users and suppliers) and their involvement in the risk assessment
- specialist professional or other knowledge required
- lessons learnt from previous similar procurements
- other context that may contribute to increased risk associated with the procurement (e.g. procurement related to emergency situations, etc.).

Step 2: Risk Identification[2]

Public authorities should identify and describe the potential risks that may impact on the achievement of the procurement objectives. This may include risks that are common to all procurement processes as well as risks that are specific to the particular procurement (i.e. the goods or service).

The source of the risk against each procurement objective should be identified, as well as the events, causes, and potential consequences on the objective.

Consider all risks, and whether they are within the control of the public authority. It can be helpful to consider two questions:

1. What can happen?
2. How and why could it happen?

Compile a list of the possible events that could have an unwanted or unintended effect on the procurement. Consider the full lifecycle of the good or service and include problems that may arise after the goods are received or during service delivery.

[2] https://www.procurepoint.nsw.gov.au/system/files/documents/guidelines_risk_management.pdf

When identifying the potential risks, it is important to involve people with appropriate subject matter knowledge. In procurements that are complex or strategic in nature, the advice and assistance of appropriately experienced and qualified experts (for example, technical specialist, risk expert, researcher or lawyer) is strongly recommended. A consultative approach with stakeholders brings together different areas of expertise in the risk management process.

Risks identified on similar projects and/or industries should be investigated through this process, to include the widest range of potential risks.

Examples of some common procurement risks is included in Procurement Services SA's Risk Assessment template.

Step 3: Risk Analysis

Public authorities should analyse the identified risks to determine the likelihood of the risk arising and the impact if the risk were to occur (consequence). This analysis can support decisions about how risks should be treated to bring them within acceptable limits for the procurement.

The analysis of likelihood and consequence may be undertaken to varying degrees of refinement, depending on the scale of potential risk and the data available. The greater the potential risk, the greater the level of analysis required.

The main questions to consider are:

- How likely is the risk event?
- What are the consequences of the risk event?

It is also important to consider the interdependencies of different risks and their sources.

When first analysing risk, assess the consequence and likelihood of the risk without consideration of any controls or treatments.

Step 4: Risk Evaluation (Assessment)

Public authorities should evaluate the identified risks to assess the overall level of impact against their **risk appetite**[3], and to make decisions about which risks need further controls, actions or treatment, and the priority and responsibility for that treatment.

There are multiple sub-processes under the Risk Evaluation (Assessment) step:

1. Assess risk (likelihood & consequence)
2. Determine inherent risk rating
3. Identify existing controls
4. Reassess risk (likelihood & consequence) following implementation of controls
5. Determine residual risk rating

[3] Risk appetite – a measure of the level of risk an organisation is willing to assume

Together, this process of comparing the results of the risk analysis with the public authority's risk appetite, helps to determine whether the risk is acceptable or tolerable.

Step 4.1 – Assess Risk

Following steps 2 and 3 (identifying and analysing risk), the overall risk level can then be determined.

In most risk management frameworks, there are four common levels of risk: **low**, **medium**, **high** and **extreme**. For example:

Level of Risk	Example	Action
Low Risk	Procurement of readily available and commonly used goods or services (e.g. office supplies).	These risks can often be accepted. Low-level risks should be managed by routine procedures, and can usually be managed by the nominated officer (such as the Sourcing Lead or Contract Manager)
Medium Risk	Procurement of commonly used goods or services, which involve a complex element such as technology or specialist knowledge (e.g. professional surveying)	These risks should be monitored and managed by routine processes, so long as the situation is constant. They should be elevated to a higher risk level if the likelihood or potential consequences increase. Medium-level risks should be assigned management responsibility.
High Risk	Procurement which involves high costs, long-term supply, innovative technology or services, or provide an essential good or service on behalf of the public authority (e.g. residential care services).	These risks should be addressed as a priority and require a specific treatment plan/risk management plan. High-level risks should be assigned management responsibility (at a minimum) and should be reported through relevant governance structures.
Extreme Risk	Procurement which involves significant complexity, high costs, long-term supply, critical technology or services, limited supply markets, or provides a critical good or service on behalf of the public authority, that the public authority would not be able to provide in the absence of this procurement (e.g. public transport services).	These risks should be avoided and require immediate action. Extreme-level risks require immediate action detailed in the risk management plan and should be assigned senior management/executive responsibility and be reported through relevant governance structures.

It is common to use a risk assessment matrix as per the example below, which plots the likelihood of the risk against the consequence, to determine the level of risk.

Example Risk Assessment Matrix (Heatmap)[4]

Consequence	Critical	High	High	Extreme	Extreme	Extreme
	Major	Medium	Medium	High	High	Extreme
	Moderate	Medium	Medium	Medium	High	High
	Minor	Low	Low	Medium	Medium	Medium
	Insignificant	Low	Low	Low	Low	Low
		Rare	Unlikely	Possible	Likely	Almost Certain
	Likelihood					

Step 4.2 – Inherent Risk Rating

The determination of the level of risk provides the **inherent risk rating**. The inherent risk represents the level of risk that *exists in the absence of controls*.

Step 4.3 –Consider Controls

Existing controls are those mechanisms that are already in place to address inherent risks. Examples of these controls include the implementation of existing policies, procedures and templates. These controls often exist to address common procurement risks, such as insufficient procurement planning, lack of probity, etc.

Step 4.4 – Reassess Risk

Following the identification of existing controls, the likelihood and consequence of the risk should then be reassessed, to determine any changes in the overall risk level.

Step 4.5 – Residual Risk Rating

The determination of the reassessed level of risk provides the **residual risk rating**. The residual risk is the amount of risk that remains *after controls are considered*.

Step 5: Risk Treatment

Risk treatment involves selecting one or more options for modifying/mitigating the residual risks and plans for implementing those treatment options. The implementation of these options may provide new, or modify existing, risk controls.

The type of risk treatment depends on the public authority's risk appetite and **risk tolerance**[5] for specific risks, level of residual risk, and its impact on the procurement objectives.

[4] The Procurement Services SA Risk Assessment template provides a number of further examples

[5] a measure of the amount of risk an organisation is capable of absorbing. Risk Tolerance will usually involve an assessment of whether to accept, avoid, transfer, or reduce the risk.

Risk treatment involves a cyclical process of:

- reassessing existing controls/treatments;
- deciding whether the level of risk is tolerable;
- if not tolerable, generating a new risk treatment; and
- assessing the effectiveness of that treatment.

The table below provides some examples of common risk treatment options available for different risk tolerance scenarios:

Risk Tolerance	Application	Treatment Options
Accept	• When the risk impact is insignificant to minor and is less than the cost of controlling or eliminating the risk. • When the risk cannot be avoided or transferred or the cost to do so is not worthwhile.	• Continue to employ existing controls and appropriate risk mitigation strategies to manage the risk. • Monitor the risk.
Avoid	• When the impact of the risk is unacceptable and must be avoided.	• Do not proceed with the activity that causes the risk. • Seek alternative ways to achieve the outcome.
Transfer	• Shift responsibility from the public authority to another party who will bear the consequences if the risk arises. The public authority may incur a cost for the other party assuming the risk. • Responsibility should be borne by the party best able to control, bear and manage that risk. • If transferring risk to another party, this must be appropriately communicated.	• Insurance policies. • Contracts/Agreements with specific terms and conditions between a public authority and its suppliers.
Reduce	• When the risk must be accepted, implement changes or alternatives to minimise the consequences and likelihood of the risk occurring.	• Clarify contract terms, requirements and specifications. • Contract management. • Revise policy and procedures and implement new ones as necessary. • Specify professional accreditation. • Upgrade supervisory requirements.

Step 6: Developing a Risk Management Plan

The purpose of a risk management plan is to identify, analyse and document risk strategies associated with the procurement.

The level of detail to be recorded and documented in a risk management plan should be commensurate with the complexity, risk profile and value of the procurement. At a minimum it is recommended that the risk management plan includes:

- information on the procurement context including the objectives, scope, procurement strategy and key stakeholders

- an outline of how risks were identified, analysed and evaluated (including extent of involvement of any experts)
- a risk assessment for each identified area of risk, including addressing the following criteria[6]:
    - a brief description of the risk (what could happen and why), which is often grouped into categories such as planning, goods/services, procurement process, industry/suppliers, management, stakeholders and contract)
    - consequences of the risk occurring that being the outcome of an event and the severity of its effect (i.e. insignificant, minor, moderate, major, critical) on the procurement objectives, and clients/end-users, employees, the public authority, suppliers and other stakeholders
    - likelihood of the risk occurring (i.e. rare, unlikely, possible, likely, almost certain)
    - evaluation and rating of the level of inherent risk (i.e. low, medium, high, extreme)
    - existing controls (existing measures or actions that modifies or regulates risk)
    - inherent level of risk (based on assessment of consequence and likelihood)
    - reevaluation of level of risk, following implementation of controls
    - residual level of risk (based on assessment of consequence and likelihood following controls)
    - options for managing the risk (risk treatment)
    - party or parties responsible for managing the risk
    - a summary of the risks escalated in accordance with the public authority's internal risk management practices including (where relevant) the public authority's Procurement Governance Committee
    - the process for how risks will be monitored, managed and reviewed on an ongoing basis.

A risk management plan should be treated as a 'live' document and regularly reviewed to monitor existing and identify new risks. Public Authorities may use Procurement Services SA Risk Management Plan template, and tailor this to ensure it is fit-for-purpose.

Step 7: Monitor and Review Risks on an Ongoing Basis

Throughout the procurement process public authorities should monitor risks and the effectiveness of any treatments. The nature of risk can change throughout the course of the procurement and the risk management plan should be regularly reviewed to ensure its ongoing relevance and amended if circumstances change.

Entering into contracts does not remove risks from the public authority in relation to

[6] https://www.hpw.qld.gov.au/__data/assets/pdf_file/0016/3355/procurementguidesignificantprocurement.pdf

the provision of the goods and/or services involved. At time, it can increase risk or introduce new risks. If the risks are not managed it may result in increased costs to the State and loss of services. The risks need to be well controlled through effective contract management practices.

Public authorities should consider the roles and responsibilities of different functions through the ongoing monitoring of risks, including:

- Public authority's Risk Management Unit
- Procurement Governance Committee
- Central Procurement Unit
- Sourcing Lead
- Contract Manager
- Subject Matter Experts

Additionally, other functions within the public authority may be required to lead, participate, or provide advice through the ongoing monitoring of risks, including: internal audit, finance units, and legal units.

Procurement Review Committee (PRC)

At the request of Cabinet, the Treasurer, Minister, or public authority Chief Executive, the PRC may review procurements deemed high-risk and make recommendations based on the outcomes of their review. This review may involve a review of the risk management practice associated with the procurement. Further information about the role of the PRC is provided in the *Procurement Governance Policy*.