

# Managing risk in procurement procedure

This is a mandated procedure under the operational policy framework. Any edits to this page must follow the process outlined on the [creating, updating and deleting operational policies](#) page.

## Overview

This procedure provides guidance in understanding risks inherent to procurement, and the components and processes involved in risk management.

This procedure outlines the necessary steps to effectively manage procurement risk and assists business units and employees to identify, assess, minimise, and monitor risks throughout the procurement process.

## Scope

The procedure applies to all corporate employees, education offices and public authorities operating within the department's procurement framework.

This procedure should be read in conjunction with the [procurement governance policy](#) and [procurement procedure](#).

School and preschool employees, school governing councils, school councils and preschool management committees should refer to the [school and preschool procurement procedure](#).



# Contents

Managing risk in procurement procedure .....	1
Overview.....	1
Scope .....	1
Detail.....	3
Risk management .....	3
Risk management in procurement.....	3
Risk management processes .....	4
Roles and responsibilities .....	10
Chief Executive .....	10
Managers.....	10
Employees .....	10
ICT assurance team.....	10
Procurement and Contracting Unit .....	10
Definitions .....	11
control .....	11
issue.....	11
risk .....	11
treatment .....	11
routine procurement.....	11
complex and strategic procurement .....	11
business unit.....	11
Supporting information .....	11
Related legislation .....	11
Related policies.....	12
Record history .....	12
Approvals.....	12
Revision record.....	12
Contact .....	13

# Detail

## Risk management

The [SA Government Risk Management Guide](#) places responsibility on agency chief executives for the effective and timely implementation of risk management standards and practices, in accordance with the Australian/New Zealand Standard AS/NZS ISO 31000:2018. This Standard defines risk as the effect of uncertainty on objectives.

A risk is a future condition or circumstance that could impact on objectives if it occurs, whereas an issue is a current event or condition that requires action to be resolved. Risk is measured by combining the consequence or impact of the event with its likelihood. This may have a positive or negative impact on outcomes.

Managing risks involves the systemic, positive identification of threats and development of appropriate strategies to manage risk. This enables the department to take appropriate action towards the management of resources.

The department takes a proactive decision-making approach that seeks to avoid or minimise risks. The Audit and Risk Directorate implements an overarching [risk management policy](#) and [risk management procedure](#) in line with across government policy. Refer to these for further information.

The managing risk in procurement procedure specifically governs risk management relating to procurement activities within the department.

## Risk management in procurement

The department takes a systematic approach to ensure risks associated with the purchase of goods or services are identified, assessed, managed, and monitored to ensure that unexpected or undesirable outcomes are minimised. Where procurement risk is well managed, project objectives are more likely to be achieved.

Where a procurement involves information or data, the risk assessment must consider information security and privacy. The department is aligned with the [South Australian Protective Security Framework](#), which provides required actions and guidance related to security risks that can occur through the lifecycle of a procurement. In line with this, the department identifies and mitigates security risks, ensures relevant security terms and conditions are included in agreements, and manages and monitors security risks for any changes that could affect the security of the department. The [ICT cyber security standard \(PDF 488KB\)](#) provides further information. Contact the ICT team at [education.ICTCyberSecurity@sa.gov.au](mailto:education.ICTCyberSecurity@sa.gov.au) for advice.

The value and risk of the procurement will determine the level of effort required to manage risk effectively.

For all procurements valued above \$55,000 (GST inclusive), a risk assessment must be completed. This will clearly identify and document the identified risks, potential impacts, likelihood and consequence of the risk, proposed mitigation and treatment strategies and the inherent and residual risk rating.

For [routine procurements](#), identified risks can be documented within the Routine Acquisition Plan. The [risk assessment template \(DOCX 43KB\)](#) can be used to document the required information.

A separate Risk Management Plan must be prepared for all [complex and strategic procurements](#) during the acquisition planning stage and accompany the acquisition plan when it is submitted for approval.

The Risk Management Plan will be completed collaboratively between the [business unit](#) and Procurement and Contracting. An effective risk management plan will include:

- the context, scope, objectives and procurement strategy associated with the project
- a summary of how the risks were identified and analysed
- a register of identified and prioritised risks required to be managed, and their assigned owner
- a statement about how the risks will be monitored and reviewed during the project.

The risks and the effectiveness of treatments should be monitored on a regular basis. The nature of risk may change throughout the course of a procurement process, and it is likely that the risk management process may need to be repeated and appropriate action taken as required. In all cases record the risks along with the applicable treatment. For further information on or assistance with managing risk in procurement, submit a request through [edProcure](#).

## Risk management processes

For all complex and strategic procurements, risk assessment and management must be documented in a Risk Management Plan and included in the Acquisition Plan submission. Consider the following key phases of risk management when undertaking a procurement process.

### Communication and consultation

Undertake communication and consultation with the relevant internal and external stakeholders throughout the process. This ensures that all stakeholders share the same understanding of risks within each procurement activity and how they are to be managed.

### Establishing the context (internal and external)

To establish the risk management context for the procurement, it is important to understand the environment in which the procurement is undertaken.

To establish the context, consider:

- legislation, policies and standards relevant to the procurement objectives
- external elements including the political, economic, cultural, and competitive environment
- the value of any information or data
- timeframes required to undertake the procurement activity
- the importance of the procurement to the business and its objectives
- the relationships with, and perceptions and values of, internal and external stakeholders
- capabilities in terms of resources such as people, processes, capital, systems and technology

- the organisation's approach to risk in terms of levels of acceptable risk
- defining responsibilities for risk management in the procurement process
- previous experience or lessons learned from similar procurements.

## Identifying risk

Identifying any risks and their associated impacts is required for all procurement activities. These may include risks specific to the procurement as well as risks common to all procurement processes. Useful tools and techniques that can be used to identify risks include:

- checklists
- brainstorming
- systems analysis
- drawing on outside experience
- strengths, weaknesses, opportunities and threats (SWOT) analysis.

Examples of common risk categories in a procurement context include:

### Planning and preparation risk examples

- unrealistic time or cost expectations
- inadequate analysis of the supply market
- conflict with existing contracts or supply arrangements
- limited capacity to access necessary information
- legal complexities
- delays in obtaining approvals
- incorrect method of approach selected.

### Product or service risk examples

- limited availability
- complex to manufacture or source
- integration of the product into existing environment
- delays in delivery, testing and installing
- unsafe use of hazardous materials or practices
- final product or service does not meet expectations.

## Procurement process risk examples

- lack of probity or unethical behaviour
- changes to scope or specifications
- proper processes are not followed
- risks are not adequately managed
- market approach process does not achieve value for money
- government policies not followed.

## Industry and supplier risk examples

- lack of interest in response to tender
- limited number of potential suppliers
- industrial disputes
- lack of capacity of individual suppliers
- complacency in long term supplier relationships
- non-performance of suppliers.

## Management risk examples

- inappropriately qualified or resourced project team
- lack of communication amongst team or facilitators
- responsibilities of project staff not clearly defined
- expectations and objectives unclear
- contract is poorly managed
- loss of corporate memory relating to contract
- unethical behaviour or conflicts of interest.

## Stakeholder risk examples

- public sensitivity or high level of media scrutiny
- conflict among stakeholders
- change in government policy or political demands
- ineffective communication and consultation
- lack of co-design and shared agreements with Aboriginal businesses/services.

## Contract risk examples

- offer lapse before execution
- errors or omissions in the contract
- default by the supplier or termination of the contract
- payments made in advance of goods or service received
- acceptance of suppliers' terms and conditions
- bank guarantees
- procurement objectives not realised
- unplanned changes to scope or technology
- lack of proper records
- mismanagement of sub-contractors
- unjustified contract extensions or amendments
- fraud.

## Information security and privacy risk examples

- unauthorised access to, or data breach or leak of, information or data causing harm to a child or young person
- breach of confidentiality
- service is not available (connectivity, backups, disaster recovery, service levels, support)
- website defacement or unauthorised modification leading to reputation damage to SA Government, the department or a site
- non-compliance with SA Government security policy or standards or DPC Circular 012: Information Privacy Principles (IPPs) instruction
- data sovereignty and cross jurisdictional legal issues with data custodianship.

## Risk analysis

Risk analysis is a process of determining why, how, and where a possible risk might occur. It involves identifying existing controls, if any, and assessing the effectiveness of those controls.

In determining the level of risk associated with procurement activities, 2 key elements require consideration:

- Likelihood – how likely is it that the potential risk will occur?
- Consequence – what will happen if the potential risk eventuates?

## Risk evaluation

Once the likelihood and consequence of the identified risks have been analysed, evaluate and prioritise the risks so that the most significant risks are treated first.

Employees must demonstrate the method by which any identified risks will be managed. The [risk assessment criteria matrix \(PDF 218KB\)](#) can assist to determine the risk area, appropriate consequence rating, likelihood of occurrence and classify the specific risks as either extreme, high, moderate or low. This will help to determine appropriate methods to regulate the risks. The [risk assessment template \(DOCX 43KB\)](#) can be used to document this information.

## Risk treatment

If existing controls are not able to manage risks to within a defined tolerance level, or when the control is ineffective, treatment may be required.

To treat a risk, select one or more options for modifying or mitigating the residual risk. Plan for implementing a treatment option. Implementation of a treatment option may provide new or modify existing risk controls.

Treating risk is a cyclical process of:

- Reassessing existing controls or treatments
- Deciding whether the level of risk is tolerable
- If not tolerable, generating a new risk treatment
- Assessing the effectiveness of that treatment.

Depending on the level of risk identified, the following risk treatment options may be considered:

- accept the risk (this may be appropriate if there is no feasible treatment option or if the impact of the risk is minimal)
- avoid the risk
- reduce the likelihood and/or consequence of occurrence
- share the risk.

## Regulating risk

Procurement and Contracting has put in place several controls to assess and manage risk throughout the procurement process. These include:

- preparing standard templates and policy documents to guide employees throughout the procurement process
- implementing procurement delegations within the department and creating the procurement governance committee to oversee high value and high-risk procurements.

## Accepting risks

Accept the risk when:

- the impact of the risk is minimal or insignificant and does not exceed the measures, financial or otherwise, required to control or eliminate the risk
- the risk cannot be avoided or transferred or the cost to do so is prohibitive.

Example risk treatment options when accepting the risk include:

- employing appropriate risk mitigation strategies to manage the risk
- managing the risk using existing procedures.

## Avoiding risks

Avoid the risk when the impact of the risk is unacceptable and must be avoided. Risk avoidance might increase the significance of other risks.

Example risk treatment options when avoiding the risk include:

- ceasing the activity affected by the risk
- seeking alternative ways to achieve the outcome.

## Reducing the likelihood or consequence of risks

When the risk has to be accepted, implement changes or alternatives to reduce the likelihood or consequence of the risk occurring.

As a guideline, the preventative actions should cost less than the expected value of exposure or less than the cost of the contingency plan.

Example risk treatment options when reducing the likelihood or occurrence of the risk include:

- reviewing contract terms and conditions, requirements, and specifications
- specifying professional accreditation
- upgrading supervisory requirements
- conducting additional project analysis
- ensuring cultural protocols are met, including co-design and consultation with Aboriginal businesses.

## Sharing risks

Transfer responsibility of the risk from the department to another party who will bear the consequences if the risk arises. Depending on the risk level, careful qualification of the third party should be undertaken and contracted in advance.

Insurance policies or contractual agreements with third parties are examples of transferring the risk.

## Monitoring risk

Undertake regular review and monitoring of the identified risks, to evaluate the effectiveness of the planned strategies for these risks. This can also identify new risks that have emerged which may impact the procurement process.

Monitoring risk reinforces the risk management process, provides information for decision making and can contribute to the achievement of the identified outcomes.

## Roles and responsibilities

### Chief Executive

Accountable for ensuring that risk management frameworks that relate to the department's business and organisational context are developed and implemented.

### Managers

Ensure employees undertaking procurement processes are sufficiently informed about relevant policies, procedures and guidelines.

Managers include, but are not limited to, executive directors, directors, education directors, assistant directors, principals, preschools directors and supervisors.

### Employees

Employees required to undertake procurements should familiarise themselves and maintain currency with relevant legislation, government, and department procurement requirements.

### ICT assurance team

Provide expert advice regarding:

- information classification (value), information security risk, controls, and treatments
- compliance with government information security frameworks, policies, standards, and regulations.

### Procurement and Contracting Unit

Monitor and evaluate the effectiveness of the procedure and conduct periodical reviews as required.

# Definitions

## control

An existing mechanism that can be verified and seeks to reduce the likelihood and/or consequence of a risk.

## issue

A current event or condition that requires action to be resolved.

## risk

A future condition or circumstance that could impact on objectives if it occurs.

## treatment

An additional mechanism to be implemented that seeks to reduce the current likelihood and/or consequence of a risk.

## routine procurement

A routine procurement is one that is classified using the Procurement Initiation Complexity tool as low to medium risk and valued above \$55,000 and up to and including \$1,500,000 (GST inclusive).

## complex and strategic procurement

A complex procurement is one that is classified as low to medium risk and valued above \$1,500,000 (GST inclusive).

A strategic procurement is one that is classified as high risk, regardless of value.

## business unit

Is a catch-all term to refer to all non-school, corporate, and ancillary functions within the department.

# Supporting information

## Related legislation

[Public Finance & Audit Act 1987](#)

[Treasurer's Instruction 18](#)

## Related policies

[Risk management procedure](#)

[Risk management policy](#)

[Procurement governance policy](#)

[Procurement procedure \(PDF 231 KB\)](#)

[ICT security risk assessment procedure \(PDF 264KB\)](#)

[DTF procurement governance policy](#)

[DTF procurement planning policy](#)

[DTF sourcing policy](#)

[DTF contract management policy](#)

## Record history

Published date: November 2023

## Approvals

OP number: 143

File number: 14/10038

Status: approved

Version: 3.1

Policy officer: Senior Project Officer, Procurement Operations

Policy sponsor: Chief Procurement Officer

Responsible executive director: Chief Operating Officer

Approved by: Chief Procurement Officer

Approval date: 9 November 2023

Review date: 9 November 2026

## Revision record

Version: 3.1

Approved by: Chief Procurement Officer

Approval date: 9 November 2023

Review date: 9 November 2026

Amendment(s): Updated contact details.

Version: 3.0

Approved by: Chief Operating Officer

Approval date: 26 October 2023

Review date: 26 October 2026

Amendment(s): Updated to implement continuous improvement opportunities, and maintain compliance with the Treasurer's Instruction 18 - Procurement and associated policies.

Version: 2.0

Approved by: Chief Operating Officer

Approval date: 21 June 2021

Review date: 21 June 2024

Amendment(s): Amended information following the rescinding of the State Procurement Act 2004 and introduction of Treasurer's Instruction 18.

Version: 1.3

Approved by: Director, Procurement and Transport

Approved date: 19 June 2019

Review date: 7 September 2021

Amendment(s): New branding applied to document, published as HTML document on EDi, edited for plain English in consultation with Communications directorate.

Version: 1.2

Approved by: Director, Procurement and Transport

Approved date: 18 January 2019

Review date: 7 September 2021

Amendment(s): Transferred to new template and updated hyperlinks.

Version: 1.1

Approved by: Director, Procurement and Transport

Approved date: 7 September 2018

Review date: 7 September 2021

Amendment(s): Minor edit – machinery of government changes and review date.

Version: 1.0

Approved by: Deputy Chief Executive

Approved date: 24 March 2017

Review date: March 2020

Amendment(s): Updated to reflect SPB's revised procurement thresholds and requirements. Change from guideline to a procedure.

Version: 4.3

Approved date: April 2015

Amendment(s): Created regulating risk section, including controls. Inserted definitions and abbreviations section.

## Contact

Procurement and Contracting

Phone: 8226 1610

[Ask your question or lodge a request through edProcure.](#)