



# Managing risk in procurement Procedure

---

## 1. Purpose

The Managing risk in procurement Procedure has been developed to assist the Department for Child Protection (DCP) staff in the identification and minimisation of risks in the procurement process.

## 2. Scope

The procedure applies to all DCP staff involved in any capacity in the acquisition of goods and services on behalf of DCP, regardless of the value of the good or service procured.

The procedure should be read in conjunction with the [Procurement Governance Framework](#), the [Risk Assessment Framework](#) and the suite of policies and guidelines governed by Procurement Services SA within the Department for Treasury and Finance (DTF).

The procedure aims to assist in developing an understanding of risks inherent to procurement, and the components and processes involved in their management. This procedure specifically targets risk management relating to the procurement activities within the department.

## 3. Authority

### 3.1 Legislative context

Not applicable.

### 3.2 Whole of Government requirements

The South Australian Government's Risk Management Policy Statement (2009) 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standards and practices, in accordance with the Australian/New Zealand Standard AS/NZS ISO 31000:2009 which has been superseded by ISO 31000:2018.

This procedure is to be read in conjunction with the risk-based framework, [South Australian Protective Security Framework](#) (SAPSF) which provides additional policy requirements relating to the identification and management of risk within protective security processes and procedures.

### 3.3 DCP requirements

- [Risk Assessment Framework](#)
- [Procurement Governance Framework](#)
- [Procurement Governance Policy](#).

## 4. Procedure requirements

### 4.1 Risk assessments and analysis in procurement processes



The level of detail and effort required to manage risk in procurement will vary depending on the nature and value of the procurement. A Complexity Assessment must be undertaken at the commencement of the procurement process to assist and guide the applicable risks associated with a procurement, by the procurement lead. The outcome of the Complexity Assessment will provide a Complexity Classification which will govern the required procurement processes. For further information on these classifications and processes, please refer to [Procurement Governance Policy](#).

Regardless of the financial value of an acquisition, where the outcome involves information and/or data, information security risk and privacy must be considered and where appropriate, included within contractual arrangements.

Examples of commonly encountered risks are included at Attachment 1. This is intended as a guide only and is not exhaustive.

#### 4.1.1 Routine procurements

A risk assessment must be undertaken and the risks documented within the acquisition plan for procurements which are considered to be a routine procurement. The risk assessment must be undertaken in accordance with the [Risk Assessment Framework](#). Routine procurements will be assigned a risk rating of low to medium risk when applying DCP's [Risk Assessment Matrix](#).

The risk assessment will include the:

- identification of the risks associated with the procurement
- potential impact/consequence of the risk
- likelihood of the risk occurring
- existing controls
- proposed mitigation and/or treatment of the risk
- residual risk rating.

#### 4.1.2 Complex / strategic procurements

Procurements which have been assessed and are considered to be complex or strategic will require a detailed risk assessment which identifies the risks, the likelihood of the risks occurring, the potential impact and proposed treatment of the risks. Assessment of the procurement is undertaken by the procurement lead. This is to be documented and included with the associated acquisition plan. The risk assessment must be undertaken in accordance with DCP's Risk Assessment Framework. Complex or Strategic procurements will have a risk rating of medium to high risk when applying DCP's [Risk Assessment Matrix](#).

Where the procurement is considered high risk (regardless of Complexity Assessment outcome), a separate risk management plan must be prepared and provided as supporting documentation to the acquisition plan.

An effective risk management plan will include:

- information including the context, scope, objectives, key stakeholders and procurement strategy associated with the project
- an outline of how the risks were identified, analysed and evaluated
- a register of identified and assessed risks.

The Risk Assessment as discussed above is to include the following information:

- a description of the risk
- the consequences of the risk



- the likelihood of the risk
- the inherent risk rating
- the existing controls
- the risk treatment
- the residual level of the risk.

Where a risk(s) has been identified as part the procurement, DCP staff should monitor the risk(s) and the effectiveness of treatments 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, there is a need to identify and maintain a record of high or extreme risks, accompanied by the applicable treatment.

## 5. Compliance, monitoring and evaluation

The risks identified throughout the procurement process may continue to be monitored and addressed throughout the life of the contract throughout annual reviews and performance reporting. The management and administration of the resulting contracts and identified risks will be undertaken in accordance with DCP's Contract Management Framework and, where applicable, Contract Management Plan.

This procedure will be reviewed and updated by Procurement and Contracting Unit in accordance with the requirements stipulated in the DCP Policy Governance Framework.

The effectiveness of this procedure will be monitored and evaluated by the Procurement and Contracting Unit as part of this process.

## 6. Related documents

Related documents, forms and templates
<a href="#">Procurement Services SA - Procurement Governance Policy</a>
<a href="#">Procurement Services SA – Procurement Planning Policy</a>
<a href="#">Procurement Services SA – Contract Management Policy</a>
<a href="#">Procurement Services SA – Risk Management Guideline</a>
<a href="#">Procurement Services SA – Complexity and Capability Assessments</a>
<a href="#">Procurement Governance Framework</a>
<a href="#">Risk Assessment Framework</a>
<a href="#">Procurement Governance Policy</a>
<a href="#">Risk Assessment Matrix.</a>

## Document control

Reference No./ File No.		
Document Owner	Lead Writer (position)	
Directorate/Unit: Procurement and Contracts, Finance and Corporate Services	Manager Procurement and Contracting	
Accountable Director: Chief Financial Officer		



<b>Commencement date</b>	11 September 2024	<b>Review date</b>	6 September 2027
<b>Risk rating</b> <a href="#">Risk Assessment Matrix</a>	<b>Consequence Rating</b>	<b>Likelihood</b>	<b>Risk Rating</b>
	Minor	Unlikely	Low

REVISION RECORD		
Approval Date	Version	Revision description
February 2018	1.0	Document published
7 May 2021	2.0	Transition to new template and minor updates
6 September 2024	3.0	Review as per policy review cycle. Changes include embedding DTF Procurement Services SA updates to Treasurers Instruction 18- Procurement, on February on 2023 and associated PSSA Policies and Procedures documents where relevant to this document.



## Attachment 1 – Identification of risks in procurement

Risk category	Examples of risks
<b>Planning and Preparation</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Unrealistic time/cost expectations</li> <li><input type="checkbox"/> Delivery</li> <li><input type="checkbox"/> Inadequate analysis of the supply market</li> <li><input type="checkbox"/> Conflict with existing contracts/supply arrangements</li> <li><input type="checkbox"/> Limited capacity to access necessary information</li> <li><input type="checkbox"/> Legal complexities</li> <li><input type="checkbox"/> Delays in obtaining approvals</li> <li><input type="checkbox"/> Incorrect method of approach selected</li> <li><input type="checkbox"/> Procurement approval not granted in time</li> <li><input type="checkbox"/> Unplanned changes to scope</li> </ul>
<b>Product/Service</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Limited availability</li> <li><input type="checkbox"/> Complex to manufacture/source</li> <li><input type="checkbox"/> Integration of the product into existing environment</li> <li><input type="checkbox"/> Delays in delivery, testing and installing</li> <li><input type="checkbox"/> Unsafe use of hazardous materials or practices</li> <li><input type="checkbox"/> Final product/service does not meet expectations</li> </ul>
<b>Procurement Process</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Lack of probity or unethical behaviour</li> <li><input type="checkbox"/> Changes to scope and/or specifications</li> <li><input type="checkbox"/> Proper processes are not followed</li> <li><input type="checkbox"/> Risks are not adequately managed</li> <li><input type="checkbox"/> Tender process does not achieve value for money</li> <li><input type="checkbox"/> Government policies not followed</li> </ul>
<b>Industry and Suppliers</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Lack of interest in response to tender</li> <li><input type="checkbox"/> Limited number of potential suppliers</li> <li><input type="checkbox"/> Industrial disputes</li> <li><input type="checkbox"/> Lack of capacity of individual contractors</li> <li><input type="checkbox"/> Complacency in long term supplier relationships</li> <li><input type="checkbox"/> Non-performance of contractors</li> </ul>
<b>Management</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Inappropriately qualified or resourced project team</li> <li><input type="checkbox"/> Lack of communication amongst team/facilitators</li> <li><input type="checkbox"/> Responsibilities of project staff not clearly defined</li> <li><input type="checkbox"/> Expectations and objectives unclear</li> <li><input type="checkbox"/> Contract is poorly managed</li> <li><input type="checkbox"/> Loss of corporate memory relating to contract</li> <li><input type="checkbox"/> Unethical behaviour/conflicts of interest</li> <li><input type="checkbox"/> The Supplier does not achieve and/or deliver on agreed objectives</li> </ul>
<b>Stakeholders</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Public sensitivity/high level of media scrutiny</li> <li><input type="checkbox"/> Conflict among stakeholders</li> <li><input type="checkbox"/> Change in government policy/political demands</li> <li><input type="checkbox"/> Ineffective communication and consultation</li> </ul>



Risk Category	Examples of Risks
<b>Contract</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Offer lapse before execution</li> <li><input type="checkbox"/> Errors/omissions in the contract</li> <li><input type="checkbox"/> Default by the supplier/termination of the contract</li> <li><input type="checkbox"/> Payments made in advance of goods/service received</li> <li><input type="checkbox"/> Contract negotiations with supplier breakdown</li> <li><input type="checkbox"/> Failure of supplier to fulfil service agreement requirements</li> <li><input type="checkbox"/> Acceptance of suppliers' terms and conditions</li> <li><input type="checkbox"/> Procurement objectives not realised</li> <li><input type="checkbox"/> Unplanned changes to scope and/or technology</li> <li><input type="checkbox"/> Lack of proper records</li> <li><input type="checkbox"/> Mismanagement of sub-contractors</li> <li><input type="checkbox"/> Unjustified contract extensions/amendments</li> <li><input type="checkbox"/> Supplier is unable to execute contract via DocuSign</li> </ul>
<b>Information Security and Privacy</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Unauthorised access to, or data breach/leak of, information/data causing harm to a child or young person</li> <li><input type="checkbox"/> Breach of confidentiality</li> <li><input type="checkbox"/> Service is not available (connectivity, backups, disaster recovery, service levels, support)</li> <li><input type="checkbox"/> Cyber attack</li> <li><input type="checkbox"/> Non-compliance with SA Government security policy/standards</li> <li><input type="checkbox"/> Data sovereignty and cross jurisdictional legal issues with data custodianship</li> </ul>