RISK MANAGEMENT PROCEDURE COR079

BACKGROUND

In accordance with the SA Government Risk Management Policy the Department has established a Risk Management Framework which comprises the:

- Risk Management Policy (COR078)
- Risk Management Procedure (COR079)
- Risk Management Rating Matrix (appendix one to COR079)
- Risk Register (appendix two to COR079)
- Risk Management Prompt Sheet (appendix four to COR079)

OBJECTIVE

The Risk Management Framework has been established to mitigate the effect of uncertainty on the Department's objectives.

The Risk Management procedure will:

- Establish a methodology for the identification, assessment and treatment of key risks;
- Support the training of Departmental staff in the use of the methodology;
- Establish a consistent and systematic approach to documenting risk management practices and reporting on risk;
- Integrate risk management into business and project planning;
- Provide assurance to the Under Treasurer that all departmental wide high and extreme risks have been appropriately identified, measured and treated; and
- Ensure all risks are appropriately treated.

SCOPE

This guide applies to all branches within DTF. It is also acknowledged that some statutory authorities are serviced by DTF employees and where relevant those entities' risk management policies and practices should reflect the intent of this policy.

RISK MANAGEMENT PROCEDURE COR079

WHAT IS RISK MANAGEMENT?

Risk management:

- is a set of coordinated activities to direct and control an organisation with regard to risk;
- contributes to the achievement of objectives and improvement of performance in, for example, project management, legal and regulatory compliance, service quality, efficiency of operations, governance and reputation. Risk management is not a stand alone activity that is separate from the main activities and processes of the organisation;
- is part of the responsibilities of management and an integral part of all departmental processes, including strategic planning, business planning, project and acquisition planning and management and change management;
- explicitly addresses uncertainty, the nature of uncertainty and how it can be addressed; and
- is a systematic, timely and structured methodology which will provide the department with consistent, comparable and reliable results.

KEY DELIVERABLES FROM THE RISK MANAGEMENT PROCESS

At Departmental Level
The Department will maintain a consolidated risk register which documents all high and extreme departmental wide risks including both strategic and operational risks. This register will be presented to the Audit and Risk Committee and Under Treasurer annually.

Risk and Audit Services (RAS) will coordinate regular training and facilitation of the risk management process.

At Branch Level
Branches will prepare a Branch Risk Register, using the methodology outlined below at least annually as part of the business planning process.

The annual Branch Risk Register is to be forwarded to RAS each year to enable the preparation of the departmental consolidated risk register which is presented to the Audit and Risk Committee and Under Treasurer.

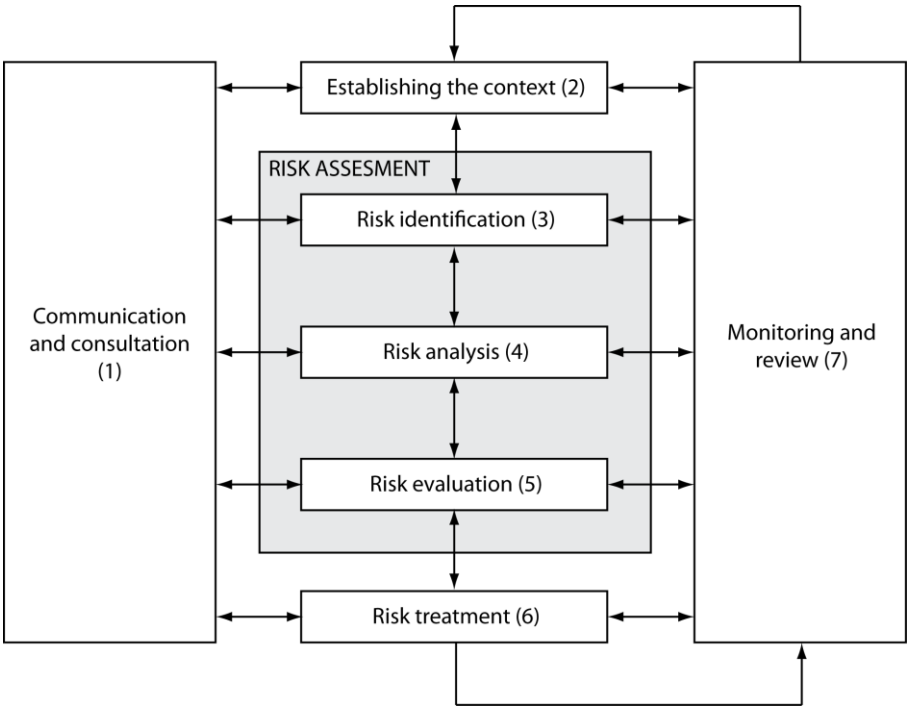
Branch Heads and the management team should monitor their risks on a regular basis and report any further high or extreme risks to RAS.

At Major Project or Activity Level
Project and Activity Managers should, at the least, prepare a list of risks and an associated action plan detailing how the risks will be mitigated and by whom. The documentation will evidence the identification, analysis and assessment of risks, and summarise existing and proposed controls.

The level and format of the documentation and reporting regime should be agreed with the Project Board/Steering Committee/Manager to ensure the risk management process is commensurate with the size/complexity/risk of the project or activity.

OVERVIEW OF THE RISK MANAGEMENT PROCESS

The Department's risk management process is shown in the following diagram:



RISK MANAGEMENT PROCESS – OVERVIEW
(AS/NZS ISO 31000:2009)

IMPLEMENTING RISK MANAGEMENT: THE 7 STEP PROCESS

For a 'Quick Guide' to the Risk Management process, refer to appendix 3.

1. Communication and Consultation

Communication and consultation with internal and external stakeholders should occur at each step of the risk management process. This ensures that those responsible for implementing risk management and those with a vested interest, understand the basis on which decisions are made and why particular actions are required.

The benefits of a consultative approach include:

- ensuring that the interests of stakeholders are understood and considered;
- helping to ensure risks are adequately identified; and
- bringing different areas of expertise together for defining, analysing, evaluating and determining appropriate treatment of risks.

Tip: It may be clear that a particular project has a large number of stakeholders with a range of interests in the project. In this case a communication and consultation plan identifying the stakeholders, who is to be consulted and by whom, when it will take place, how the process will occur and how it will evaluated may be of assistance. For large projects a risk identification workshop may be helpful.

2. Establishing the Context

The next step in the risk management process is to establish the context in which the risk assessment will occur. There are a number of elements to this step.

Establishing the external context
The external context is the external environment in which the Department, Branch or project operates. Establishing the external context involves gaining an understanding of the external environment within which the risk identification, assessment and treatment options are considered. The external context can include, but is not limited to:

- the political, legal, regulatory, financial, technological, economic and competitive environment;
- key business drivers; and
- relationships with, and perceptions and values of external stakeholders.

Establishing the internal context

The internal context is anything within the Department, Branch or project that can have an effect on the achievement of objectives. Establishing the internal context involves gaining an understanding of the internal environment within which the risk identification, assessment and treatment options are considered. The internal context can include, but is not limited to, consideration of:

- governance, organisation structure, roles and accountabilities;
- relevant policies, objectives and strategies;
- availability of resources and knowledge of staff;
- information systems and decision making processes; and
- relationships with, perceptions and values of internal stakeholders.

Establishing the context of the risk management process

The objectives, strategies, scope and parameters of the Department or the part of the Department where the risk management process is being applied, should be established.

Establishing the context of the risk management process may involve:

- setting the risk appetite;
- establishing the goals and objectives of the risk management activities;

- defining responsibilities for and resources required within the risk management process;
- specifying the nature of decisions that need to be made; and
- identifying the relationship between the project, process or activity and other projects, processes or activities within the Department or Branch.

Defining risk criteria

The Department has defined risk criteria to be used to evaluate the significance of risk. This is documented in the Risk Management Rating Matrix (appendix 1).

Risk Assessment
Risk Assessment consists of the next three steps:

3. Risk Identification

The aim of this step is to establish a comprehensive list of events which could effect the achievement of objectives. It is useful to ask the following questions in relation to the achievement of objectives: "What can happen, where and when?" and "Why and how it can happen?" All risks and potential risks should be identified and documented, including the source and impact of the risk/event and their causes and potential consequences.

Examples of techniques for identification of risk exposures include:

- Brainstorming as groups or individuals;
- Interview sessions with staff, either individually or in groups;
- Questionnaires or checklists;
- Scenario (or "what if") analysis; and
- Lessons learned.

This step also serves to confirm the completeness and validity of previously identified risks having particular regard to the current internal and external context.

It is often useful to group risks into a number of generic categories to assist with risk identification and to ensure that key risks are not overlooked. Examples of generic potential risks and sources of risk are included in the risk management prompt sheet (appendix 4). The categories are not mutually exclusive and risks may fit in more than one of them. Alternatively, other risks might be identified that do not fit into any of the categories.

At the end of this step you will have a list of unprioritised risks ready to be assessed. These can be entered in the Risk Register (appendix 2).

The number of risks identified will vary depending on the nature of the Branch or project, and the extent of detail that is preferred for the risk plan being prepared. However, it is better to identify too many risks at this point, as they can be quickly prioritised in the next steps of the process to a more manageable number.

Tip: If you are having trouble getting started, perhaps get out last year's plan, or a previous project, and identify objectives that were not achieved as planned, or opportunities that were missed. In many cases the underlying cause for why this happened will continue to be a risk for future years or projects. RAS can also provide assistance.

4. Risk Analysis

Risk analysis involves developing an understanding of the risks which have been identified.

Risk analysis requires consideration of the following steps:

1. What is the **cause/source** of the risk?
2. How **likely** is it that the risk will eventuate?
3. What will be the **consequence** should the risk eventuate?
4. What **controls** are currently in place to mitigate this risk and how effective is the control?
5. What is the **residual risk rating** (risk rating after current effective controls/treatments)?

In this process the likelihood simply means "what probability is there of the event occurring?" and consequence means "how serious will the outcome of the event be to the Branch/ Department/ project?"

There are several methods used to analyse risk, the most simple and often most appropriate being the qualitative analysis. Qualitative analysis uses words to describe the magnitude of potential consequences and likelihood that those consequences will occur. The Department has established a Risk Management Rating Matrix (appendix 1) to assist with the analysis of risk.

Having undertaken this step, the original list of risks will now:

- be understood as to what the source or driver of the risk is;
- have a listing of current controls in place to mitigate the risk; and
- be rated according to the likelihood of the risk eventuating and the magnitude of the consequence should the risk eventuate.

Note: It is good practice to document the inherent risk for each identified risk as part of the risk identification process. Inherent risk is the risk which exists in the absence of any action to control or modify the circumstance.

5. Risk Evaluation

Based on the outcome of the risk analysis, the purpose of the risk evaluation is to make decisions about which risks need to be treated and the priority for treatment implementation.

Risk evaluation involves comparing the level of risk found during the analysis process (residual risk rating) with the risk appetite established when the context was established. Based on this comparison, the need for treatment can be determined.

In simple terms, “given our risk appetite, can the risk be accepted or do further controls/strategies need to be implemented to mitigate the risk?”

If the residual risk is greater than the Department/Branch/Project’s risk appetite a risk treatment plan should be established.

Depending on the circumstances, the risk evaluation can lead to a decision to:

- undertake further analysis;
- implement additional controls; or
- not treat the risk any further.

Risks should be rated in order of priority for treatment so that the risk management process can be conducted in a systematic and cost effective way.

Tip: When evaluating and prioritising risks, it is a good idea to think about the monitoring process. How you prioritise the different risks should correlate to who they are reported to and who will manage the risk (ie: what should be reported to the Under Treasurer/Audit Committee/Branch Head as opposed to a Project/Line Manager).

6. Risk Treatment

The next stage involves selecting the most appropriate treatment option/s and implementing the selected treatment/s. Once implemented, treatments provide or modify the controls.

Risk treatment is a cyclical process consisting of:

- Assess the risk treatment;
- Decide whether residual risk levels will be tolerable; and
- If the residual risk is not tolerable, devise a new risk treatment.

Options to treat risk can include the following:

- Implementing measures to reduce the likelihood and/or consequences of the event;
- Establishing an appropriate risk treatment plan;
- Avoiding the risk by deciding not to proceed with the activity;
- Accepting and retaining the risk (by informed decision and with appropriate reporting); or
- Transferring the risk to another party.

Risk treatment options need not be mutually exclusive, many risk exposures will benefit from more than one option. The potential success might be increased when considered in combination.

It is necessary to consider the cost of implementing a risk treatment option against the benefits derived to ensure that the benefits are not outweighed by the cost of implementation.

The purpose of a risk treatment plan is to document how the preferred treatment option will be implemented. The treatment plan should further reduce the residual risk in line with the risk appetite of the area under review. Risk treatment plans should be approved by an appropriate authority prior to implementation.

Within the Department, the risk treatment plan will generally be contained within the Risk Register and should document:

- The preferred treatment option;
- Proposed actions to implement the treatment option;
- Those accountable for approving and implementing the plan;
- Reporting requirements; and
- Due date for implementation.

7. Monitoring and Review

Branches are required to report all high and extreme risks identified on their Branch Risk Registers to RAS.

RAS will prepare a consolidated risk register for the department which will be reported to the Audit and Risk Committee and Under Treasurer annually.

Branches should establish their own monitoring and review process based on their risk appetite. Responsibility for monitoring and review should be clearly defined. The branch risk monitoring and review process may take place at regular management or project meetings, or may be scheduled in at periodic times.

The monitoring and review process should include all aspects of the risk management process to ensure:

- Controls are effective and efficient (both in design and control);
- Lessons and information from events (near misses) are captured to strengthen the process for managing risk;
- Changes in the internal and external context are identified and the risk register is adjusted as appropriate; and
- Emerging risks are identified on a timely basis.

The results of this process should be recorded and reported to appropriate officers.

Guidance for reporting risk:

- Extreme Risk – Immediate action required, develop a specific risk treatment plan, the Under Treasurer, Branch Head and RAS should be made aware
- High Risk – Risk treatment plan should be a priority – Branch Head and RAS should be made aware
- Moderate Risk – Management responsibility should be specified

- Low Risk – Manage by routine procedures, nominated officer should monitor

Tip: Setting up and communicating this step early in the process can be a key driver in ensuring its overall success. Once people understand how the information will be used they are more likely to have more commitment to each of the steps.

DOCUMENTING THE PROCESS

Adequate supporting records need to be maintained to evidence the department has complied with the SA Risk Management Policy and Treasurer's Instruction 2.

In most cases this will involve completing the Department's Risk Register template (appendix 2), however, the documentation should support the process, rather than drive the process.

Documentation should be commensurate with the size and complexity of the process being analysed.

RELATED DOCUMENTS

- SA Government's Risk Management Policy Statement;
- Risk Management Policy (COR078)
- AS/NZS ISO 31000:2009 Risk management - Principles and guidelines
- Risk Management Prompt Sheet
- Risk Management Matrix
- Risk Register

CHIEF OPERATING OFFICER

6 / 12 / 2016

Negative Consequence			Likelihood						Opportunity
			A **Rare** (In exceptional circumstances) Frequency: Beyond once every 5 years	**B** **Unlikely** (Could occur at some time) Frequency: Up to every 5 years	**C** **Possible** (Might occur at some time) Frequency: Up to once per year	**D** **Likely** (will probably occur in most circumstances) Frequency: Up to six monthly	**E** **Almost Certain** (expected to occur in most circumstances) Frequency: Up to once per month		
5 (Critical)	• Death of staff, financial loss in excess of $1 million, destruction or serious damage to most assets • Royal Commission / Widespread national media exposure • Key service delivery interruption for greater than one week • Breach of governing legislation	**M**	**H**	**H**	**E**	**E**	• Major initiative with long term benefit to government or the community • Initiative which significantly reduces risks to the government or the community	**1** (Critical)
4 (Major)	• Injury to staff, loss of critical mass of staff, financial loss up to $1 million, destruction or serious damage to key physical or information assets • Parliamentary inquiry / Widespread State Media exposure • Key service delivery interruption for greater than 1 day • Breach of non-governing legislation	**L**	**M**	**H**	**E**	**E**	• Major initiative with long term benefit to DTF • Initiative which significantly reduces risks to DTF	**2** (Major)
3 (Moderate)	• Permanent loss of key staff, financial loss up to $500,000, damage to physical or information assets • Ministerial question in Parliament / State media • Key service delivery interruption for greater than half a day • Failure to comply with policy	**L**	**M**	**M**	**H**	**E**	• Major initiative with long term benefit to the Branch • Initiative which significantly reduces risks to the Branch	**3** (Moderate)
2 (Minor)	• Temporary loss of key staff, financial loss up to $100,000 • Minor media exposure • Minor service delivery interruption • Failure to comply with guidelines	**L**	**L**	**L**	**M**	**H**	• Initiative with benefits within the Branch • Initiative which reduces risks within the Branch	**4** (Minor)
1 (Insignificant)	• No staff impact, financial loss up to $10,000 • Potential for public interest • Minor service interruption which does not affect overall service delivery • Failure to comply with internal instructions	**L**	**L**	**L**	**L**	**M**	• Initiative with small short term benefit • Initiative which reduces minor short term exposure	**5** (Insignificant)

E: Extreme Risk – Immediate action required with specific risk treatment plan Under Treasurer, Branch Head and RAS should be made aware
H: High Risk – Risk treatment plan should be a priority –Branch Head and RAS should be made aware
M: Moderate Risk – Management responsibility should be specified
L: Low Risk – Manage by routine procedures – Nominated Officer should monitor

FYXX INSERT BRANCH NAME Risk Register – SUMMARY PAGE

Risk ID	Risk Description	Risk Level	Responsibility
HEADING 1 (Eg: Financial Risks)			
1.			
2.			
3.			
HEADING 2 (Eg: Operational Risks)			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

FYXX INSERT BRANCH NAME Risk Register - DETAIL

ID	Risk Description (what could happen which will impact on the department achieving its objectives?)	Current Controls (how do we currently manage this risk?)	Impacts (Impact on department's objectives if risk eventuates)	Residual Risk			Risk Treatment Plan	
				L	C	Risk Level	**Additional Controls/Mitigation Strategy to be implemented** (Further controls to reduce risk rating)	Responsibility / Due Date
Heading 1 (eg: Strategic Risks)								
1.		•	•				• It will assist in monitoring implementation if additional controls are specific actions which can be measured.	
2.		•	•				•	
Heading 2 (eg: Financial Risks)								
3.		•	•				•	
4.		•	•				•	

Government of South Australia
Department of Treasury and Finance

Quick Step by Step Guide to Completing a Risk Register

The purpose of this document is to provide a step-by-step guide to completing a risk register. Please refer to the Risk Management Procedure (COR079) for more detailed explanations. Alternatively Risk and Audit Services can provide assistance.

1 Establish the Context

Understand the external context (ie: economic, legal, regulatory, etc) and the internal context (governance, org structure, IT systems etc).

- Define the objectives, strategies, scope and risk appetite of the part of the organisation where the risk management process is being applied.
- Define responsibilities and resources required.
- Determine the level of documentation required based on the size and complexity of the area being reviewed.

2 RISK ASSESSMENT

a. Risk Identification

The purpose of this step is to establish a comprehensive list of events which could effect the achievement of the objectives defined above.

Potential risk identification techniques:

- Brainstorming as groups or individuals;
- Questionnaires or checklists;
- Scenario (or "what if") analysis; and
- Lessons learned.

Refer to the Risk Management Prompt Sheet for examples of generic risks (appendix 4).

Document all the (unprioritised) risks identified, including the source and impact of the risk and the risk's causes and consequences in the Risk Register (appendix 2).

b. Risk Analysis

The purpose of this step is to develop an understanding of each risk identified at step two.

Consider the cause and source of the risk, the consequence and the likelihood the consequences will occur. Using the risk criteria determine the level of residual risk after considering current controls in place, the interdependence of risks and any assumptions made. Refer to the DTF Risk Management Rating Matrix (appendix 1)for DTF criteria.

Agree and document the final list of risks, the risk rating and controls for each risk in the Risk Register.

c. Evaluate the Risks

Compare the residual risk (RR) to the risk appetite to identify which risks require a risk treatment plan and priority reporting.

3 Treat the Risks

Risk treatment is a cyclical process:

- Assess the risk treatment;
- Decide whether RR levels will be tolerable;
- If the RR is not tolerable, devise a new risk treatment.

Options to treat risk include:

- Implementing strategies to reduce the likelihood and/or consequence;
- Establishing a risk treatment plan;
- Avoiding the risk;
- Accepting and retaining the risk; or
- Transferring the risk to another party.

Consider the costs and benefits of each option. Select the most cost effective option and document how the chosen treatment option will be implemented (actions required, by whom, due date, reporting requirements).

4 Monitor the Risks

Monitoring and review should be planned and regular. Clearly define responsibilities for monitoring and reviewing risks. This process should include:

- Ensuring controls are effective;
- Lessons learned;
- Detecting changes to the context;
- Identifying emerging risks; and
- Process improvements.

The results of this process should be recorded and reported.

APPENDIX 4 – RISK MANAGEMENT PROMPT SHEET

Risk Management Prompt Sheet

Examples of generic risks

The first step in a successful risk management program is the accurate and complete identification of risks. It is important to use a structured and systematic process when identifying risks.

Examples of techniques for identification of risk exposures include:

- Brainstorming as groups or individuals;
- Interview sessions with staff, either individually or in groups;
- Questionnaires or checklists;
- Scenario analysis ('What, why and how can a risk occur?'); and
- Lessons learned.

This sheet provides some examples of generic risks and/or causes that can provide a starting point for establishing a register of risks. Branches need to use the above techniques to identified risks specific to their operations. This list may be useful, for example, in identifying risks as part of the overall business planning process. Other prompt sheets such as the procurement prompt sheet will assist for more specific projects.

The categories set out below are not mutually exclusive and risks may fit in more than one of them. Alternatively, other risks might be identified that don't fit into any of the categories.

1. Strategic and Stakeholder

- Our ability or inability to achieve government or departmental objectives
- Significance changes to the internal or external environment (economic, social, political etc)
- Our ability to maintain stakeholder confidence and manage stakeholder expectations
- Our ability to manage change (ie: change in Government priorities)
- Mis-use of confidential information

2. Organisational Governance

- Management of the culture and values
- Changes to planning and reporting processes
- Implementation of delegations and accountability for decision making
- The development and application of policies
- Management of intellectual property

3. Asset and Financial Management

- Financial systems
- Budget and funding processes
- Managing revenue
- Managing our costs
- Controls and audit processes
- Fraud and Corruption Prevention
- Probity and ethics
- Contingency planning
- Recording and managing assets

4. Human Resources

- Attraction and retention of staff
- Managing staff performance
- Induction and training

5. Health, Safety and Environment

- Hazards and injuries
- Bullying and harassment of staff
- Managing contractors
- Major incident impacting business continuity
- Complying with legislation

6. Legal

- Compliance with legislation, policies and standards
- Managing legislative change
- Identifying and managing indemnities and liabilities

7. Information Technology

- The way we manage and store information
- The way we use information
- The way we use and manage our knowledge
- Security of systems and information

8. Program and Project Delivery

- The way we plan and manage programs and projects
- The way we acquire goods and services
- The way we engage and manage consultants and contractors
- Contract Management
- Probity and ethics in our dealings