SA Government
Risk Management Guide

Risk management is about understanding and managing the risk environment and taking measures to ensure those risks are contained to acceptable levels.

The South Australian Government (SA Government) is committed to ensuring effective risk management remains at the core of its activities. Agencies should aim to embed risk management in decision-making, organisational culture and processes to contribute to the achievement of the strategic objectives of the agency and the SA Government.
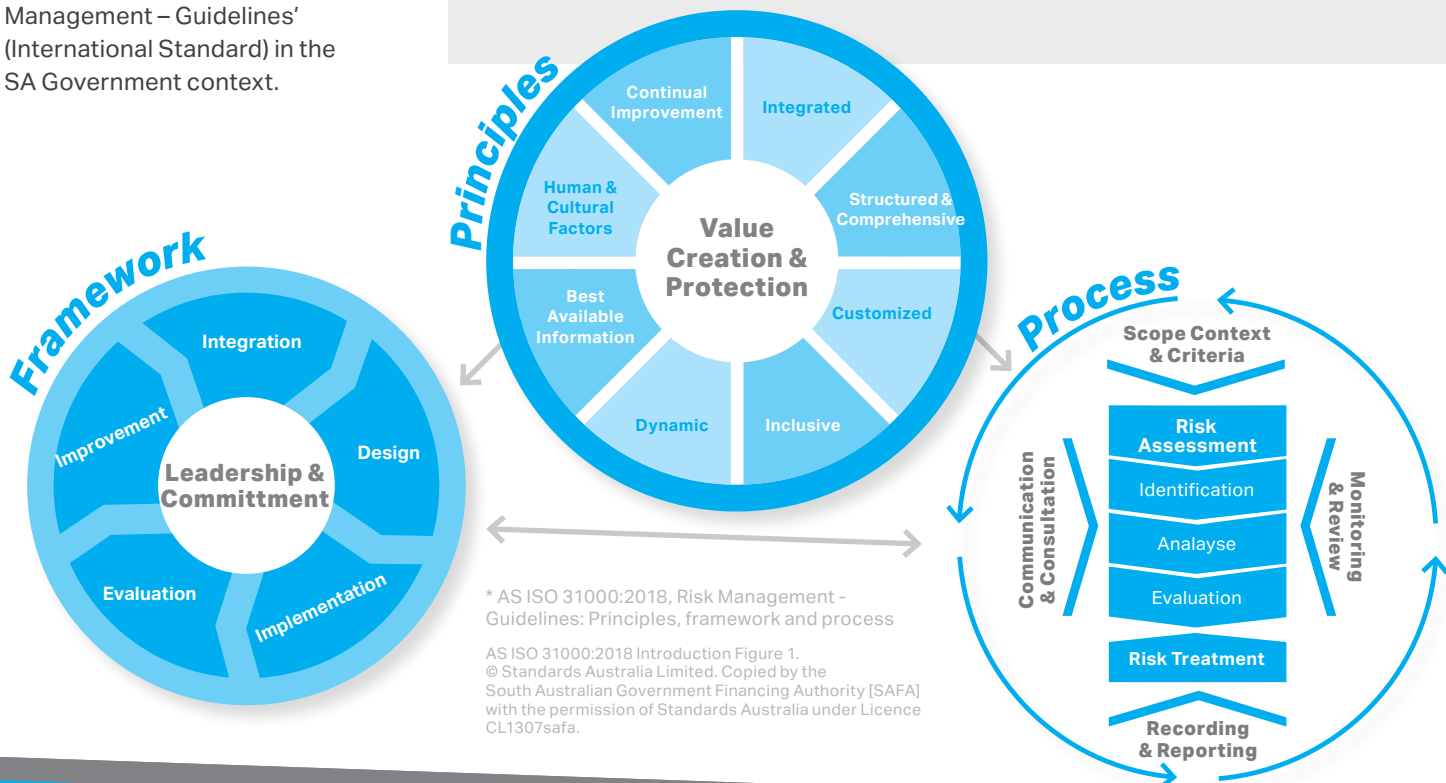
This better practice guide will assist agencies in the adoption of the International Standard AS ISO 31000:2018 'Risk Management – Guidelines' (International Standard) in the SA Government context.

Purpose of Risk Management
Value Creation and Protection

The International Standard defines the purpose of risk management as 'the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives'. This creation and protection of value occurs at all stages of government and agency management, including:

- policy development and decision making
- setting, achieving and delivering objectives
- adapting to change and identifying opportunities and innovation
- reviewing and improving performance.

To support this, risk management activities should be integrated at all stages of agency management and in all agency activities in a manner which is structured and customised to each agency. Risk management approaches should be inclusive of all information available to stakeholders and be dynamic and responsive to a changing information and operating environment. Effective risk management should also seek to leverage available human, technological and other resources to drive continuous improvement or take advantage of opportunities.

Framework

Leadership & Committment
- Integration
- Design
- Implementation
- Evaluation
- Improvement

Principles

Value Creation & Protection
- Continual Improvement
- Integrated
- Structured & Comprehensive
- Customized
- Inclusive
- Dynamic
- Best Available Information
- Human & Cultural Factors

Process

Scope Context & Criteria
- Risk Assessment
  - Identification
  - Analyse
  - Evaluation
- Risk Treatment
- Communication & Consultation
- Monitoring & Review
- Recording & Reporting

* AS ISO 31000:2018, Risk Management - Guidelines: Principles, framework and process

AS ISO 31000:2018 Introduction Figure 1. © Standards Australia Limited. Copied by the South Australian Government Financing Authority [SAFA] with the permission of Standards Australia under Licence CL1307safa.

SAFA
South Australian Government Financing Authority

Government of South Australia

www.safa.sa.gov.au

Elements of Risk Management

The following elements are considered better practice for risk management in the SA Government context.

- **Develop a Positive Risk Culture**
- **Define Risk Appetite**
- **Risk Management Framework**
- **Risk Management Process**
- **Responsibility & Oversight**
- **Capability & Reporting**
- **Integrated Risk Management**

Develop a Positive Risk Culture

Risk culture is the system of shared values and behaviours that drive the decision making of management and employees. It reflects the influence of organisational culture on how risks are managed. An effective risk culture is one that proactively enables and rewards staff to make well informed risk decisions.

The below management actions will support the development and implementation of risk management within the agency by ensuring:

- commitment to risk management is effectively communicated from the top of the agency
- the operational structure of the agency facilitates effective risk management
- the need to integrate risk management into all aspects of the agency is reinforced.

A targeted and structured approach to cultural change should be adopted by:

Identifying the current state of risk culture

Determining the targeted level of risk culture acceptable within the entity

Developing strategies focused on achieving the targeted level

Monitoring and reviewing the strategy.

Define Risk Appetite

Develop an appropriate, clear and concise risk appetite statement that addresses the agency's material risks. By developing a risk appetite statement to guide decision makers, the agency is able to make more nuanced and informed decisions.

The risk appetite statement should convey:

- the degree of risk the agency is prepared to accept in pursuit of its strategic objectives (risk appetite)
- for each material risk, the maximum level of risk that the agency is willing to accept, expressed as a risk limit and based on its risk appetite (risk tolerance)

- the process for monitoring compliance with each risk tolerance and for taking appropriate action in the event that it is breached
- the timing and process for review of the risk appetite and risk tolerances.

Risk Management Framework

The agency's risk management framework enables appropriate development and implementation of strategies, policies, procedures and controls to manage risk that are customised to the unique requirements of the agency.

The Risk Management Framework should include the following elements:

- the agency's purpose for managing risk and links to agency objectives
- the need to integrate risk management into the overall culture of the agency
- processes for identifying and assessing risks and controls
- processes for establishing, implementing and testing mitigation strategies and control mechanisms
- risk matrix and guidance on likelihood and consequence
- communicating and reporting of risk issues
- the process for review of the Risk Management Framework.

Policies and procedures should be supported by systems or other tools to enable effective risk management, such as the risk management process and risk reporting.

Risk Management Process

The risk management process is a systematic approach used to identify and manage risk and defines how the agency performs integrated risk management activities. It implements the key framework elements including the risk policy, risk appetite and risk matrix.

This process is an integral part of management and decision making and should be integrated into the structure, operations and processes of the organisation. It can be applied to strategic, operational and project levels. Key elements of the risk management process are:

Being clear on the purpose of the risk process

- refer to the agency's objectives throughout the process

- define the agency's objectives by type (Strategic, Operational, Project, etc.)
- consider who should be involved and what historic and current information is available to inform the process.

Undertaking the process

- identify and describe risks, causes, consequences and controls
- conduct sessions with stakeholders systematically, iteratively and collaboratively drawing on the collective knowledge of the group based on the best available information
- assess risk at the inherent, current and target levels, through the use of consensus or voting tools, based on the defined risk matrix.

- assign responsibility to owners of risks, controls and treatment plans
- decide whether controlled risk levels are acceptable in the context of risk appetite or require further treatment
- reduce risk, where required, through treatment plans
- escalate the risk where all available resources cannot reduce the risk to an acceptable level.

Review and report on the process

- communicate risk reporting to senior leaders and the oversight board or committee
- review risks, controls and treatment plans regularly to validate the process
- establish processes to add, change or delete risks and identify new and emerging risks.

Responsibility & Oversight

Establishing a governance structure, such as boards or committees, will provide oversight of risk management in the agency.

Boards and committees should:

- oversee the operation of the Risk Management Framework
- approve or endorse the agency's risk appetite statement
- form a view of the risk culture in the agency and the extent to which that culture supports the agency's ability to operate within risk appetite
- ensure that risks are adequately considered when the agency's objectives are being set
- understand the risks and opportunities facing the agency in pursuit of its objectives
- ensure that systems to manage risks are implemented and operating effectively
- ensure that risks are appropriate in the context of the agency's objectives
- ensure that information about risks and their management is properly communicated.

Capability & Reporting

To ensure the success of risk management, the agency should invest in people and processes.

Ensure adequate risk management training, resources and tools are provided.

Establish clear risk communication, escalation and reporting processes.

Define responsibility and accountability for managing risk.

Agencies should consider dedicating a risk management function that:

- is responsible for assisting the agency, through its oversight committee and senior management, to maintain the Risk Management Framework
- is appropriate to the size, business and complexity of the agency
- is led by a senior officer who has a direct reporting line to the Chief Executive and direct access to the oversight committee
- is resourced with staff who have clearly defined roles and responsibilities and who have appropriate experience and qualifications to exercise those responsibilities
- has access to all aspects of the agency that have the potential to generate risk, including information technology systems
- is required to notify the oversight committee of any significant breach or material deviation from the Risk Management Framework.

Integrated Risk Management

Risk management activities should be integrated at all stages of agency management and in all agency activities in a manner which is structured and customised to each agency.

The following activities and practices are recommended to support integration of risk management:

- business planning at strategic, operational and project levels supported by consideration of risk which explicitly considers value created and protected

- decision making which focuses on the highest impact activities and opportunities and is guided by a risk appetite equally informed by value creation as it is by value protection

- practices which encourage and support the identification of opportunities and innovation and acceptance of upside risk without overemphasis of downside risk

- established processes to regularly monitor progress in achieving and delivering objectives and the status of relevant risks

- processes to review agency performance with the view to continuously improving practices to manage risk and extract and leverage further opportunities

- activities to capture new and emerging information and embed this within planning, decision making and review processes.

Further References

AS ISO 31000:2018 Risk Management – Guidelines

Treasurer's Instruction 2 – Financial Management

Financial Management Toolkit

Public Sector Act 2009

Terms of Reference - Guidance for Risk and Performance Committees

Glossary of Terms

Agency's Objectives – statements or goals that indicate what is critical in an agency's strategy. May be strategic, operational, project or another type of objective.

Business Plan – a document setting out an agency's future objectives and strategies for achieving them.

Risk – the effect of uncertainty on objectives. This effect could be a positive or negative deviation from what is expected.

Control – any measure or action that modifies or regulates risk. Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk.

Treatment Plan – plan to select and implement options for addressing risk. Further controls may result from the successful implementation of the plan.

Risk Appetite – the level of risk that an agency is prepared to accept in pursuit of its objectives before action is deemed necessary to reduce the risk level.

Likelihood – the probability that the risk will occur.

Consequence – the potential severity of the risk if it occurs.

Risk Matrix – a matrix used in risk assessment to define the level of risk by considering the likelihood and consequence of a risk occurring. Commonly represented as a 5x5 matrix with colours visually representing low, medium, high and extreme levels as defined by the agency.

Inherent Level of Risk – the level of risk in the absence of controls.

Current Level of Risk – the level of risk given the current state of the control environment.

Target Level of Risk – the level of risk that the agency views as acceptable.