An Overview of the Risk Management Process

Audience

This information sheet is intended to assist Commonwealth officials at the Foundation and Generalist levels. It outlines the steps of the risk management process, including:

- Identification, analysis, evaluation and treatment of risks,
- Communication and consultation,
- Monitoring and review, and
- Recording and reporting

At a glance

The risk management process described in *AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines* is one way of achieving a structured approach to the management of risk. Consistently implemented, it allows risks to be identified, analysed, evaluated and managed in a uniform and focused manner.

ISO 31000 recommends that risk management be based on three core elements:

- A set of principles that describes the essential attributes of good risk management, which support the creation and protection of value;
- A risk management framework that provides a structure for risk management within an entity or activity that is underpinned by leadership and commitment; and
- a risk management process that prescribes a tailored, structured approach to understanding, communicating and managing risk in practice.

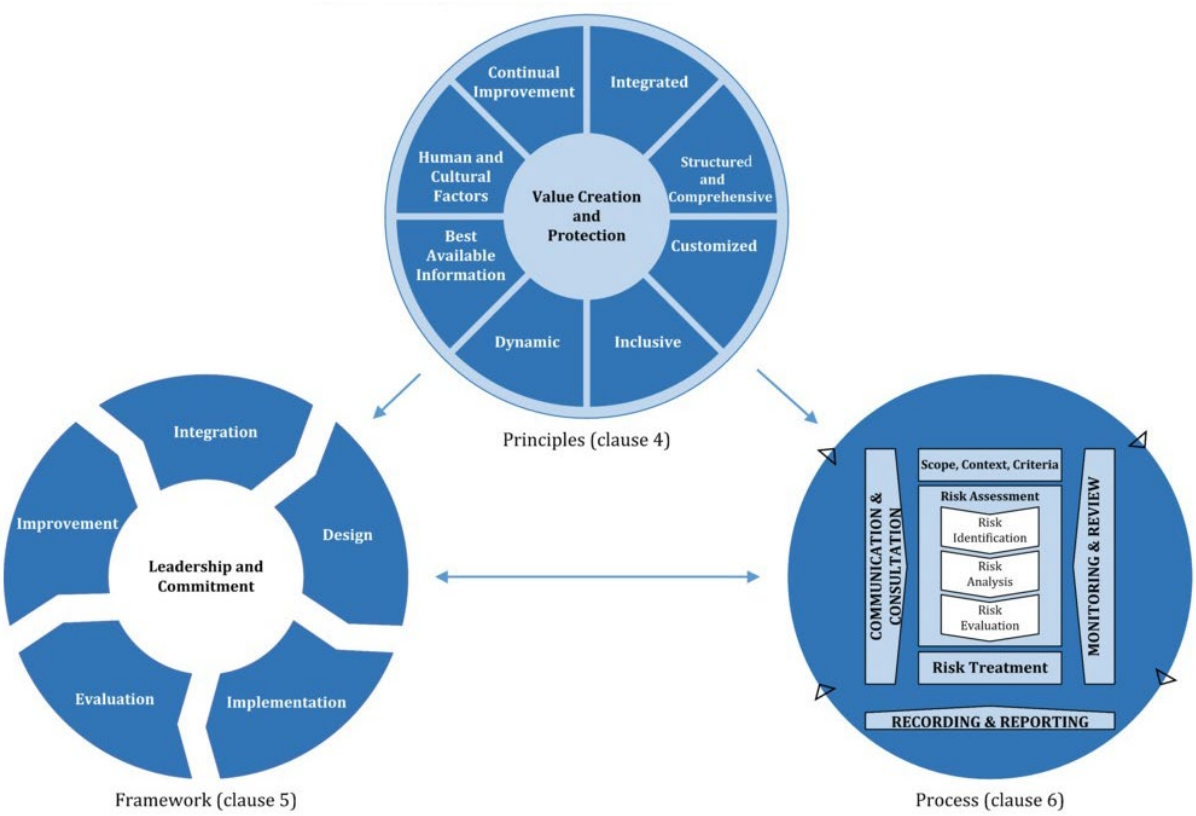

Diagram 1: Source - IS0 31000:2018 Risk Management Principles and Guidelines

The steps of the risk management process

Establish the scope, context and criteria

In order to understand and manage risk, it's first necessary to understand your entity's objectives and operating environment. Establishing the scope, context and criteria are the first of the eight risk management steps where the objectives and influences of the risk management process are defined.

The first activity is to define the scope, which involves agreeing on the objectives of the entity or the activity being considered. Objectives can include those which are both explicit (those objectives that are well defined, for example 'we will increase client satisfaction feedback by five percent') and implicit (those objectives that might be undocumented but are expected, for example 'we will obey the law'). It is also important to consider outcomes, inclusions/exclusions, resourcing requirements and relationships with other projects.

Secondly, it is important to consider the internal and external context:

- **The external context** - the environment in which the entity operates and seeks to achieve its objectives including policy, operational, cultural, social, political, people, environmental, legal, regulatory, financial, technological and economic factors. Other things to be

considered include key drivers and trends that impact upon the objectives, and the relationship with, and expectations of, external stakeholders.

- **The internal context** - includes those factors within the entity that may impact the achievement of the activity. Factors typically considered in the internal context include the entity's strategic objectives, organisational capabilities and culture.

Understanding the context also requires identifying relevant stakeholders. The most important stakeholders include organisations which may expose the entity to risk, are exposed to an entity's risks, or be able to help an entity manage risk.

The final step is to define its risk criteria by specifying its risk appetite and tolerance relative to objectives. This should be aligned with the entity's risk management framework, take into account the scope and context, and be consistently communicated within the entity.

Risk identification

The aim of this step is to develop a comprehensive and tailored list of uncertain future events in the future that are likely to have an impact (either positively or negatively) on the achievement of the objectives these are the risks.

Risks need to be documented including key elements such as the potential cause and consequence should the risk be realised.

Thorough exploration and identification of potential risks is critical to the success of any risk assessment. It is important not be too narrow or constrained. Often referred to as a 'failure of imagination', care needs to be taken to ensure that the identification process does not just focus on today's challenges but rather also considers a diverse range of sources including risk events that are emerging or in the future.

It is important to consider actions, scenarios, events and other external agencies that may give rise to risks. For each risk identified ensure that its source or cause is well understood and documented.

A number of techniques can be used during risk identification and assist in the discovery process. These can be sophisticated and highly structured, or more informal, depending on the purpose and context of the assessment being undertaken. Common techniques include the use of risk categories or linking risks to each objective identified in the context setting phase. Another method is to begin thinking of the threats and opportunities the entity faces, and use these to identify relevant risks.

Risk analysis

Risk analysis rates the potential impact of each risk and its likelihood of occurrence. The combination of these two factors determines the severity of the risk, which may be positive or negative. Although there are many ways to achieve this, a common approach is to use a matrix or 'risk heat map'. Consequence and likelihood are plotted on the two axes of the matrix, with each corresponding cell assigned a level of severity. Illustrated below is an example of a simple risk severity matrix.

Residual Risk Severity					
Likelihood/ Consequence	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Medium	Medium	High	High	Extreme
Likely	Medium	Medium	Me 9	5 12 6	Extreme
Possible	Low	Me 11	Me 3	High	High
Unlikely	Low	Low	Me 4	Me 1	High
Rare	Low	Low	L 10	Me 8	7 2

The specific matrix employed would likely be defined in an entity's risk management framework and should be considered and agreed in the 'establish the scope, context and criteria' step.

Whilst entities may use different processes for analysing risk, it is important that each entity ensures all risks within its organisation are assessed consistently. Where risks are shared between organisations, good communication is required to ensure each stakeholder understands the ownership and severity of the risks.

Risk evaluation

Risk evaluation determines the tolerability of each risk. Tolerability is different from severity. Tolerability assists to determine which risks need treatment, and their relative priority, by comparing the severity of the risk against the level of risk you are willing to accept.

At its simplest, an entity might decide that risks above a certain severity are unacceptable, and risks below this are tolerable. More sophisticated approaches might assign risk acceptance delegations for risks of increasing severity to officials of different levels of seniority.

Decisions on tolerability should also be made after considering the broader context of the risk including the impact of the risk upon other entities outside of the organisation. Treatment decisions should consider financial, legal, regulatory and other requirements. Ultimately though, the considered and informed acceptance of risk supports decision making and is essential to entity performance including the achievement of objectives.

Risk treatment

Risk treatment is the action taken in response to the risk evaluation, where it has been agreed that controls in place are deemed ineffective and additional mitigation activities are required.

Risk treatment is an ongoing process where individual risk treatments (or combinations of treatments) are assessed to determine if they are adequate to bring the residual risk levels to a tolerable or appropriate level. If not, then new risk treatments are generated and assessed until a satisfactory level of residual risk is achieved.

Risk treatment will be most effective where it is tailored to the requirements and capabilities of the entity and can include strategies such as:

- Avoiding the risk entirely by not undertaking the activity
- Removing a source or cause of the risk
- Sharing the risk with other parties
- Retaining the risk by informed decision
- Taking more risk to achieve certain objectives or opportunities
- Changing the likelihood and/or consequence of the risk through modifying controls in place.

Selecting the most appropriate treatment requires balancing the cost and effort of implementation against the benefits derived from additional risk mitigation. In some cases, further treatment may be unachievable or unaffordable and the residual risk may need to be accepted and communicated. Entities may wish to consider how external stakeholders can provide support when developing treatment options or if treatments can be implemented collaboratively.

Risk treatments are commonly documented in a risk treatment plan. These can include:

- reasons for treatment selection, including expected benefits and potential hazards
- accountabilities for approving the plan and responsibility for its implementation
- resource requirements
- reporting, assurance and monitoring requirements
- priorities, timing and schedules.

Communication and consultation

Communication and consultation is an essential attribute of good risk management. Risk management cannot be done in isolation and is fundamentally communicative and consultative. Hence this step is, in practice, a requirement within each element of the risk management process.

Formal risk reporting is only one form of risk communication. Good risk communication generally includes the following attributes:

- encourages stakeholder engagement and accountability
- maximises the information obtained to reduce uncertainty
- meets the reporting and assurance needs of stakeholders
- ensures that relevant expertise is drawn upon to inform each step of the process
- informs other entity processes such as corporate planning and resource allocation.

Different stakeholders will have different communication needs and expectations. Good risk communication is tailored to these requirements.

Monitoring and review

Risks change over time and hence risk management will be most effective where it is dynamic and, evolving and responsive. Monitoring and review is integral to successful risk management and entities may wish to consider articulating should articulate who is responsible for conducting monitoring and review activities.

Key objectives of risk monitoring and review include:

- detecting changes in the internal and external environment, including evolving entity objectives and strategies
- identifying new or emerging risks
- ensuring the continued effectiveness and relevance of controls and the implementation of treatment programs
- obtaining further information to improve the understanding and management of already identified risks
- analysing and learning lessons from events, including near-misses, successes and failures

Monitoring and review can be both periodic and/or based upon trigger events or changing circumstances.

The frequency of the review process should be commensurate with the rate at which the entity and its operating environment is changing.

Recording and reporting

The risk management process is most effective when well documented and shared. It may be included in formal risk reports to be recorded and published internally and externally as appropriate and should also be used as an input to reviews of the whole risk management framework.

Key objectives of recording and reporting include:

- Communicating risk management activities and outcomes
- Inform corporate planning and decision making
- Improve risk management activities
- Assist interaction with stakeholders

Reporting should consider the information needs of stakeholders and usefulness of information for corporate planning and decision-making.

Further information

This information sheet provides a high level overview of the risk management process. For more detailed guidance on undertaking the risk management process in practice, refer to the Comcover Information Sheet *Undertaking the Risk Management Process.*

Contact

If you have any questions or feedback in relation to this information sheet please contact Comcover Member Services at comcover@comcover.com.au.

Use of this guidance

Comcover's series of Risk Management Information Sheets are designed to be used as optional guidance documents and are not mandatory.

It is important that entities develop risk management frameworks and systems that are tailored to the needs of their organisation. Entities may choose to adapt some or all of the concepts contained in this information sheet to suit their specific needs or use alternative methodologies.