ARPI

Australian Risk Policy Institute

Guide to the Commonwealth ‘Risk Management’ Policy

2018

The Australian Risk Policy Institute (ARPI) is incorporated under the Australian Capital Territory Associations (Incorporation) Act 1991 and is a nationally registered Association under the Commonwealth Corporations Act 2001, with offices in Canberra and Melbourne.

Information regarding ARPI’s Purpose, Governing Board, Publications, Partners and Contacts appears at www.arpi.org.au.

ABN 39 120 269 534

About the Australian Risk Policy Institute

The Australian Risk Policy Institute (ARPI) is an independent, non-political and not-for-profit association created to promote Risk Policy as part of leadership, decision-making, policy formulation and assurance.

Working with academic, professional, public, corporate and community partners, ARPI promotes Risk Policy as a means of better addressing today's challenges.

ARPI's purpose is to:

- contribute to the development and adoption of Risk Policy;
- ensure a Risk Policy approach is understood and articulated; and
- comment on Risk Policy issues, including public policy and legislation.

It is important to note that ARPI is about Risk Policy - a strategic Policy approach and new thinking about Risk, that better connects leaders with Risk and at an earlier point in time than their indirect engagement with the traditional risk management processes during the life of a risk - that is, ARPI's Risk Policy approach is independent and separate from the processes of 'risk management' or managing existing risks.

More information about ARPI, including access to the (down-loadable) Risk Policy Model (2012) and Strategic Risk Policy (2016) plus a variety of publications, submissions and papers, can be found at www.arpi.org.au.

Guide to the 'Commonwealth Risk Management Policy' - Disclaimer

Please Note: This paper has been prepared by an ARPI Associate who is a Chief Risk Officer and wishes to offer suggestions on how the Commonwealth's Risk Management (Operational) Policy could be more effective from a risk management perspective. Thus the views expressed focus on risk management.

ARPI's Risk Policy Model and Risk Policy thinking, approaches and frameworks on the other hand, are quite different from and apply before the process of risk management comes into play, that is, before risks have been identified. If vulnerabilities thus identified through ARPI's Risk Policy Model approach cannot be fully protected against, risks may arise but they are likely to be fewer in number and less severe. ARPI's Risk Policy approach is now a separate professional discipline.

Table of Contents

Element One – Establishing a risk management policy

Description (Commonwealth Risk Management Policy)

A risk management policy links the entity's risk management framework to its strategic objective. Communicating the accountabilities, responsibilities and expectations within an entity's risk management policy is important to ensure a common understanding of risk across the entity.

Requirement

An entity *must* establish and maintain an entity specific risk management policy that:

a. defines the entity's approach to the management of risk and how this approach supports its strategic plans and objectives;
b. defines the entity's risk appetite and risk tolerance;
c. contains an outline of key accountabilities and responsibilities for managing and implementing the entity's risk management framework; and
d. is endorsed by the entity's accountable authority.

ARPI Guidance

See **Attachment A** - Model Risk Management Policy

An internal policy is a mechanism for establishing a control framework of rules, processes, responsibilities, procedures etc - required to control risks to the policy objective. This is the concept of risk based policy development.

Consequently a risk management policy should establish the controls necessary for achieving effective risk management within an entity. The Commonwealth Risk Management Policy requires entities to establish risk management policies with specific inclusions because these are considered as key controls for the risks to effective risk management. That is how the Commonwealth mandates controls to Commonwealth entities.

- Defining the approach to risk management *responds to the risk* that risk management is inconsistently applied within an entity
- Establishing how the approach to risk management supports the strategic plans and objectives *responds to the risk* that risk management is not integrated into the governance framework
- Defining the risk appetite and risk tolerance *responds to the risk* that the balance between the likelihood and consequences of risk (risk level) is accepted by risk owners in isolation from Executive guidance or knowledge
- Outlining the key accountabilities and responsibilities for managing and implementing the entity's risk management framework *responds to the risk* that key implementation activities are not undertaken
- Obtaining endorsement by the entity's accountable authority *responds to the risk* that there is low level senior executive (accountable authority or board) support for risk management

Entity's may identify additional risks to successfully implementing risk management and include controls (rules, processes, responsibilities, procedures, etc) for these risks in their risk management policy. Such risks may include:

- Failure to effectively report on risks
- Failure to collect risk data
- Failure to integrate risk management into other business management processes

Element Two – Establishing a risk management framework

Description (Commonwealth Risk Management Policy)

A risk management framework is the set of components and arrangements that provide the foundations and organisational approach for designing, implementing, monitoring, reviewing and continually improving risk management throughout the entity.

Requirement

An entity *must* establish a risk management framework which includes:

a. the overarching risk management policy (Element One);
b. an overview of the entity's approach to managing risk;
c. how the entity will report risks to both internal and external stakeholders;
d. the attributes of the risk management culture that the entity seeks to develop, and the mechanisms employed to encourage this;
e. an overview of the entity's approach to embedding risk management into its existing business processes;
f. how the entity contributes to managing any shared or cross jurisdictional risks;
g. the approach for measuring risk management performance; and
h. how the risk management framework and entity risk profile will be periodically reviewed and improved.

The risk management framework must be endorsed by the entity's accountable authority.

ARPI Guidance

This element of the Commonwealth Risk Management Policy aims to establish a framework for the application of risk management as a process (such as the ISO 31000 Risk Management Standard). However the specific requirements go further than process and move towards business management and governance, implying Enterprise-wide Risk Management (**ERM**).

The ERM framework at **Attachment B** combines risk management policy objectives with the application of risk management within the entity's business management arrangements, defining and enabling ERM within the organisational constructs of the entity.

The framework describes:

a. how the risk management policy supports the application of risk management
b. how risk management is applied against categories of business objectives – the entity's approach to managing risk.
c. How risk reporting forms part of the application of risk management – specific details can be included in the risk management policy
d. The internal control environment – often overlooked by entities
e. How risk management supports the business processes underpinning the achievement of objectives
f. Consideration of whole of government context with respect to control of risk

This model ERM framework is based on the COSO[1] ERM framework and should be used as guidance by entities on how to use the information generated by the assessment, control and monitoring of risks to business objectives, to better understand the relationships between the components of the business management system that they have established.

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Element Three – Defining responsibility for managing risk

Description (Commonwealth Risk Management Policy)

The accountable authority of an entity is responsible for an entity's performance in managing risk. The responsibility for the day-to-day management of risk lies with officials at all levels.

Requirement

Within the risk management policy, the accountable authority of an entity *must* define the responsibility for managing risk by:

a. defining who is responsible for determining an entity's appetite and tolerance for risk;
b. allocating responsibility for implementing the entity's risk management framework; and
c. defining entity roles and responsibilities in managing individual risks.

ARPI Guidance

Responsibility for managing risk must be defined in the risk management policy. The policy will establish risk management responsibilities for key categories of authority within the entity. For example the CEO/Secretary will have defined responsibilities with respect to risk management within the entity, as will all SES levels and Executive Level Managers. Responsibilities of all staff may also be defined in the risk management policy.

An entity's risk management policy should also establish the approach to and responsibility for, risk appetite statements and risk tolerance levels. These concepts are still developing within organisations and will change over time as their understanding and application improve. For example, initially entities may choose to establish risk appetite statements and risk tolerance levels for strategic or material risks. Over time this may be expanded to divisional or branch level risks and even individual business unit risks.

Responsibility for implementing the risk management framework should also be established in the risk management policy. However with respect to the risk management framework, Commonwealth entities should consider adoption of the Three Lines of Defence model of business assurance as part of their risk management framework.

Commonwealth entities should make their own enquiries and decisions on the appropriateness of the Three Lines of Defence model for their organisations. However the model is a very useful driver of risk management within organisations, requiring:

1. First line functions to manage risk to their business objectives
2. The second line function to deliver effective risk management within the entity including a challenge role to ensure risk is part of key business and strategic considerations (CRO)
3. The third line to provide independent assurance on the effectiveness of governance, risk management, and internal controls within the entity (audit)

Responsibility for implementation of the risk management framework sits naturally with the second line of defence.

Element Four – Embedding systematic risk management into business processes

Description (Commonwealth Risk Management Policy)

The objective of effective management is to improve organisational performance.

Considering risk is an integral element of the overall management capability of an entity and must include, and not be limited to, each of the following: strategic planning; the establishment of governance arrangements; policy development; programme delivery; and decision-making.

Requirement

Each entity *must* ensure that the systematic management of risk is embedded in key business processes.

ARPI Guidance

Element four seeks to lay the foundations for enterprise-wide risk management. ERM integrates the risk management processes undertaken in an entity with organisational design, planning, policy development and review, project and program management, and decision making. The elements below are a consequence of ERM but can also be explicitly included in the risk management policy

- Organisational Design – Organisational units/functions control risk, that is their purpose. For example the ICT function ensures that there is not a 'Failure of ICT capability to support business requirements'. This is an operational risk facing all Commonwealth entities and should be included as such in the register of operational risks. By identifying the strategic, business and operational risks facing a Commonwealth entity, the accountable authority can decide whether to create business units to manage these risks or include them in the responsibilities of existing business units.

- Planning – Planning processes should include consideration of risk. Undertaking a risk assessment of a business or project objective will engage stakeholders, identify and analyse risk, and establish controls to manage risks. Plans can then be used as the mechanism for implementing these controls. This is risk-based planning and when applied embeds risk management into the key business process of planning.

- Policy Development – A policy is a mechanism for establishing a control framework of rules, processes, responsibilities, procedures etc - required to control risks to the policy objective. Similar to risk-based planning, risk assessments can be undertaken against the policy objective. The policy is then used as the mechanism for implementing the rules, processes, responsibilities, procedures, etc) required to control risks to the policy objective.

- Project and Program Management – Risk based project planning builds the project plan using the output of a risk assessment against the project deliverable. In addition to including controls to manage risks to the project deliverable, the project plan can also include controls for project management risks such as scope, time, cost, quality, communications, human resources, procurement and integration.

- Decision Making – Decision makers need as much information as possible to make the best decision. This should include information on the likelihood of success of the proposal or decision. Such information comes from a risk assessment, informing the view on whether the risks to the proposal or decision can be managed. Further, decision makers should also be provided with an analysis of both the intended and unintended consequences of the proposal or decision. This should include an assessment of the capability to manage the anticipated intended and unintended consequences of the proposal or decision.

Element Five – Developing a positive risk culture

Description (Commonwealth Risk Management Policy)

Risk culture is the set of shared attitudes, values and behaviours that characterise how an entity considers risk in its day-to-day activities.

A positive risk culture promotes an open and proactive approach to managing risk that considers both threat and opportunity. A positive risk culture is one where risk is appropriately identified, assessed, communicated and managed across all levels of the entity. Such a culture needs to be fostered and practised by each entity.

Requirement

An entity's risk management framework *must* support the development of a positive risk culture.

ARPI Guidance

There are many drivers of risk culture within a Commonwealth entity. This includes:

- Involvement in risk assessments
- Risk based planning
- Risk based policy development and review
- Project management risk assessments
- Active business continuity
- Application and understanding the Three Lines of Defence model of assurance
- Enterprise-wide Risk Management in play
- Involvement in risk reporting

When enterprise-wide risk management and the Three Lines of Defence model combine they create one of the most effective drivers of risk culture within an entity. ERM supports business units better understand the relationship between what they do and control of organisational risk whilst the Three Lines of Defence model empowers business units to take control of risks to their business objectives, better understand how their current processes and procedures control risk and embed new control activity into business plans and individual role statements.

Further through undertaking risk assessments at the business unit level, team members are provided with a structured approach to identifying and assessing risk to their business objectives and given the opportunity to raise additional risks and new, innovative controls.

One responsibility that should be included in the risk management policy is that of monitoring the risk culture and taking steps to address any deficiencies identified. This is a key responsibility and Commonwealth entities should consider assigning it to an appropriate level in the organisation.

Entities are also encouraged to consider explicitly defining the internal control environment, or working environment in which their organisation achieves its business objectives. This takes in elements of staff satisfaction often considered through staff surveys, but also includes other elements of internal control within components such as purpose, commitment, capability and, monitoring and learning. Whilst these elements are often implicitly managed by experienced and capable managers, explicitly defining them, measuring their effectiveness and making plans to improve their performance improves the business management system, making it more resilient and sustainable whilst also contributing to the overall risk culture within the entity.

Element Six – Communicating and consulting about risk

Description (Commonwealth Risk Management Policy)

Communicating and consulting about risk underpins the successful management of risk.

Effective communication requires consultation with relevant stakeholders and the transparent, complete and timely flow of information between decision makers.

Requirement

Each entity *must* implement arrangements to communicate and consult about risk in a timely and effective manner to both internal and external stakeholders.

ARPI Guidance

The risk assessment process outlined in the ISO 31000 Risk Management Standard includes the explicit engagement of stakeholders as part of the risk assessment process. It is expected that all government agencies will reference this standard with respect to their risk assessment processes.

Stakeholders bring a range of experiences and perspectives to risk management that contributes to a robust and well considered risk assessment. This applies not only to identifying risks that may affect the achievement of an objective but also the controls that may be effective in managing risks.

Risk assessment workshops are an effective way of engaging stakeholders for the purpose of identifying risks and controls. The risk assessment process, if appropriately conducted, provides excellent structure for this engagement. It is important that the facilitation of such workshops creates an environment that enables all participants to contribute their perspectives on risks and controls without undue influence from other participants. In this regard, the use of an experienced and capable facilitator is recommended.

Entities should consider publishing, at least internally, the risk reports that are provided to executive committees including the Audit Committee, Risk Committee, ICT Committee, etc. Such reports are (or should be) high level reports on the risks and risk levels in respect of specific objectives, and may also include specific control issues that are being experienced or have been addressed. The example report below demonstrates this type of report and provides useful information to governance committees whilst also allowing entities to communicate to internal and/or external stakeholders on the management of risk within the organisation.

Objective:	**Minimise Internal Fraud**				
Risk	**Previous Risk Level**	**Current Risk Level**	**Risk Level Trend**	**Overall Control**	**Issues**
Failure to prevent fraud	**High**	**High**	↓	G	• Fraud awareness training commenced for all staff • APS values sessions conducted within business units
Failure to detect fraud	**Medium**	**Medium**	→	G	• Monthly credit card reconciliation completed • Asset stocktake commencing
Failure to respond to fraud	**Medium**	**Medium**	↑	G	• Fraud investigation services procured for another 12 months • Alignment review of types of fraud and APS code of conduct

Element Seven – Understanding and managing shared risk

Description (Commonwealth Risk Management Policy)

Shared risks are those risks extending beyond a single entity which require shared oversight and management. Accountability and responsibility for the management of shared risks must include any risks that extend across entities and may involve other sectors, community, industry or other jurisdictions.

Requirement

Each entity *must* implement arrangements to understand and contribute to the management of shared risks.

ARPI Guidance

The concept of shared risk is one that government agencies will need to consider at an agency and cross agency level. Sharing risk can include:

- Sharing the benefits of controlled risks
- Sharing the responsibility for implementing controls
- Understanding the totality of a control framework, within which risks are being managed and what role the agency plays.

If we look at business of government, we see a complicated system of roles and responsibilities, policies and programs, capabilities and networks designed to support the maintenance and growth of the Australian economy to meet the expectations of the Australian community. It is inconceivable that one Commonwealth entity is not relied upon by other Commonwealth entities to deliver their functions, objectives and purpose. Nor that a breakdown or poor performance by one Commonwealth entity does not affect the performance of other Commonwealth entities. This element encourages Commonwealth entities to look more broadly at system of government, understand their role in that system and their relationship with the role of other Commonwealth entities. Flowing from this is the opportunity to more effectively work together on a systems basis.

The Australian Risk Policy Institute's (**ARPI**) *Risk Policy Model* introduces new concepts that precede and supplement the application of traditional risk management by encouraging a paradigm shift recognising a new view of the world. Risk Policy uses the concepts of Vulnerability and Prevention as precursors to Systemic Risks and Wicked Problems to facilitate earlier warnings and decision making before any risks are identified. ARPI's Risk Policy also advises that the traditional risk management equation is no longer applicable as is and requires Policy instruction on when Consequence must for good reason dominate the equation.

The supplementary *Strategic Risk Policy* publication promotes the whole-system approach, models behaviour that may be adopted in long-reach risk environments (those situations outside the immediate reach of your organisation, whether by legal/contractual or financial means) as well as more traditional short-reach risk environments. In doing so, it emphasises the value of assessing the vulnerabilities of relevant systems. In turn, this might lead to the development of transparent information flows and cooperative approaches which minimise vulnerabilities by ensuring whole system health.

Commonwealth entities are encouraged to read and understand the concepts that ARPI is putting forward in its two publications which are available and downloadable free on the ARPI website at www.arpi.org.au:

- Risk Policy Model
- Strategic Risk Policy Model

Element Eight – Maintaining risk management capability

Description (Commonwealth Risk Management Policy)

Effective risk management requires an entity to maintain an appropriate level of capability to manage its own risk management programme and to manage its risks. The nature and scale of this capability must be considered in the context of the entity's current resource and capability profile and be commensurate with the characteristics and complexity of its risk profile.

Requirement

Each entity *must* maintain an appropriate level of capability to both implement the entity's risk management framework and manage its risks.

ARPI Guidance

The requirement that entities maintain an appropriate level of capability to manage its risks, is a broader capability requirement that is the responsibility of both the risk management function and the Human Resource (**HR**) function. The risk management function supports business units identify, assess and develop control frameworks for risks to their functions and objectives. The HR function supports business units by having effective recruitment, retention and development programs that recruits and/or produces effective leadership, technical and decision-making capability. This is an example of a shared risk within an organisation.

With respect to an entity's risk management framework, an agency should establish a dedicated risk management function whose responsibility includes establishing, maintaining and supporting risk management practices throughout the organisation. This function should be led by a Chief Risk Officer with recognised authority and appropriate risk management skills and capabilities.

By implementing Three Lines of Defence Model of Business Assurance, Commonwealth entities can appropriately focus their risk management capabilities to maximise the assurance of current and future business performance due to the effectiveness of their risk management.

- All managers in an agency are responsible for achieving the objectives and deliverables of their business unit. This includes responsibility for controlling risks to those objectives and deliverables. Whilst this is normally achieved through traditional management activity, it is significantly improved through the structured identification, assessment and control of risk (risk management). This represents the First Line of Defence within the Three Lines of Defence Model of Business Assurance. It is also relevant that reporting on risks to objective can only occur when risk management has been effectively undertaken.

- Given the specialised nature of the risk management process (ISO 31000) it is not practical to equip every manager with the skills necessary to perform the risk assessment process (although this may occur over time). It is more effective to have a specialised risk management function that supports managers to apply their and their staffs' understanding of their business function to the process of risk identification, analysis, control and reporting. This represents the Second Line of Defence within the Three Lines of Defence Model of Business Assurance.

- A risk based audit program (internal and external) that reviews a targeted and rolling program of business functions and activities, through a systematic analysis of risks and controls is another risk management capability that entities should maintain and cultivate. The assurance provided by such a program confirms (or not) that managers have identified the risks to their business functions and activities, and have implemented appropriate controls for those risks. This supports broader assurance that the entity's risk management framework is working effectively in a practical way. This represents the Third Line of Defence within the Three Lines of Defence Model of Business Assurance.

Element Nine – Reviewing and continuously improving the management of risk

Description (Commonwealth Risk Management Policy)

Formalising and implementing risk management within an entity is not a ‘one-off event’. The effective management of risk is a process of continuous improvement, requiring regular review and evaluation mechanisms.

Requirement

Each entity *must* review its risks, its risk management framework and the application of its risk management practices on a regular basis, and implement improvements arising out of such reviews.

ARPI Guidance

The requirement for an entity to review its risks is fundamentally different to the requirement to review its risk management framework and the application of its risk management practices. Although related, these are two distinct requirements.

Review of the Risk Management Framework should be embedded in the responsibility of the organisation’s Risk Committee, who should be forming an opinion of the effectiveness of the risk management framework based on:

1. The quality of the risk reports presented to the Risk Committee
2. The operation of the Second Line of Defence
3. Risk based audit reports
4. Specific review by an independent source

The Risk Committee Charter and the Risk Management Policy are the most appropriate mechanisms to establish an agency’s commitment to review of its Risk Management Framework, which should include as a minimum a comprehensive review of the risk management system every 5 years by an independent and appropriately skilled person.

With respect to the ongoing and regular review of risks, an entity ultimately achieves this through the implementation of the Three Lines of Defence model of Business Assurance. The Model embeds the provision of regular and ongoing assurance of risk control, into the normal business management practices of managers and business units. Such assurance can only be provided when risk management is being effectively applied.

When Enterprise-wide Risk Management (**ERM**) is operating effectively then the functions and objectives of business units (First Line of Defence) are viewed as risks to the higher level organisational objectives if they are not delivered or if their delivery is impaired. Under the Three Lines of Defence model of Business Assurance, business unit managers are responsible for monitoring and reporting on the control framework that supports the delivery of each business objective. Based on this understanding, managers are then in a position to assess the level of risk presented to the relevant higher level organisational objective by their business objective not being delivered.

ERM is an important concept to implement within Commonwealth entities because it allows accountable authorities, senior executives, managers at all levels and staff to better understand the relationships between objectives throughout the organisation. However, more importantly, it enables organisations to monitor all the risks within an organisation and report in a concise but strategically aligned way on the management of those risks, where ever they may reside.

Risk Management Policy

<Date>

Document Control

Version	
Status	
Authority	
Author	
Date of enactment	
Date for review	
Previous versions	

Title

Risk Management Policy

Policy Statement

<*Organisation Name*> will rigorously apply risk management principles and practices across all aspects of its business operations.

Purpose

To ensure that <*Organisation Name* > identifies and manages risks to the achievement of objectives at all levels of the organisation and uses risk management techniques in the business processes of the organisation.

Scope

The scope of this policy includes all aspects of <*Organisation Name*>strategic, business and operational objectives.

Objectives

1. To create an organisational culture where risk management is integrated with general management processes moving towards a risk based management system
2. To ensure risk management information is appropriately escalated
3. To establish and maintain organisational resilience and capability
4. To improve governance, planning and the quality of decision making throughout <*Organisation Name*>

Policy Details

Risk Governance

The Board of <*Organisation Name*> will establish a Risk Committee (*or equivalent*) to assist the Board Members to discharge their responsibilities as laid out in the Board Charter. This assistance involves:

- monitoring <*Organisation Name*> strategic, business and operational level risks
- monitoring <*Organisation Name*> risk management framework, risk governance, risk management and control processes; and
- providing the Board with assurance that <*Organisation Name*> will achieve its strategic, business and operational objectives through the systematic and rigorous application of risk management supported by efficient and effective control processes.

Risk Assessment

Risk assessments will be conducted by <*Organisation Name*> employees to support the achievement of objectives for which they have responsibility. These assessments will be based on the risk management processes detailed in the International Standard for Risk Management: 31000:2009.

Staff will be provided with training and ongoing support in the application of these risk management processes.

Each risk assessment process will be tailored to meet the context in which risk management is being applied. All identified risks will have a risk level assigned based on the Risk Level Matrix below.

Risk Level Matrix				
LIKELIHOOD	**CONSEQUENCE**			
	Severe	Major	Moderate	Minor
Almost Certain	Extreme	Extreme	Very High	High
Likely	Extreme	Very High	High	Medium
Possible	Very High	High	Medium	Low
Unlikely	High	Medium	Low	Low

A likelihood and consequence matrix must be developed for each risk assessment to define what each level of likelihood and each level of consequence means in relation to the objective against which the risk assessment is being conducted. This supports the practical application of the risk appetite statement below.

Risk Appetite

<*Organisation Name*> will not accept risks with a risk level of Very High or Extreme and requires all risks to be controlled so that no risk levels are greater than High.

Risk Escalation

When current risk levels are assessed as Very High or Extreme, the employee responsible for the objective against which the risks are identified, must notify/escalate this issue to the next level of management/governance. ie Team Leader, Manager, General Manager, CEO, Board.

It is expected that such notification will include detail on what is being done in response to the situation or what needs to be done to bring the risk level down to an acceptable level.

Risk Reporting

Reporting against risks will occur as part of normal performance reporting processes throughout the chain of command. A template for risk reporting is at **Appendix A.**

To support the monitoring and reporting of risk, a risk register will be established to record risk management information generated from risk assessments. The risk register will record risk management information against objectives at a strategic, business and operational level in line with the Risk Management Framework.

Risk Management Framework

The application of risk management within <*Organisation Name*> will be guided by a risk management framework.

<*Organisation Name*> Risk Management Framework will establish the approach to applying risk management within the governance and business management structures of the organisation. Further it will define the internal control environment - the environment in which the business management structures operate.

Corporate Policies

<*Organisation Name*> will use corporate policies as a mechanism for establishing control frameworks for key risks. Such policies will define the processes, procedures, activities and other mechanisms required to control risks to the policy objective.

Roles and Accountabilities

Role	Responsibility
Board	Establishing the policy for risk management Responsible for <*Organisation Name*> strategic risks Setting <*Organisation Name*> risk appetite
Risk Committee (*or equivalent*)	Monitoring <*Organisation Name*> strategic, business and operational level risks Monitoring <*Organisation Name*> risk management framework, risk governance, risk management and control processes, and the provision of assurance to the Board regarding their efficiency and effectiveness
Chief Executive Officer (*or equivalent*)	Promulgating the risk policy throughout the organisation and establishing a culture of risk management Ensure all strategic, business and operational level risks have an owner Provision of a regular risk management report to the Board and/or Risk Committee against <*Organisation Name*> key risks
General Managers	Promulgating the risk policy throughout the organisation and establishing a culture of risk management Provision of risk management reports to the CEO Escalating risks where the risk levels are outside tolerance levels
Chief Risk Officer	Ensuring the efficient and effective application of risk management across all aspects of <*Organisation Name*> business operations Monitoring and review of the risk management policy and framework, supported by regular (minimum of quarterly) reporting to the Executive Committee (*or equivalent*) Provision of support to <*Organisation Name*> employees in the application of risk management Maintenance of and the provision of reports from, the risk register
All Managers	Applying the risk management policy Escalating risks where the risk levels are outside tolerance levels Regularly monitoring compliance with and the effectiveness of, controls established for risks they are responsible for (including corporate policy)
All Employees	Identifying, managing and reporting on risks to objectives for which they have responsibility, including the escalation of risks when risk levels rise and control issues exist. Complying with the risk management policy Complying with risk controls as required

Evaluation and Review

The risk management policy and framework will be formally reviewed by an external party every 5 years. This review will provide an opinion on the extent to which the risk management policy was complied with and the effectiveness and efficiency of the risk management framework.

Authority

Signature

<Name and Position>

<Date>

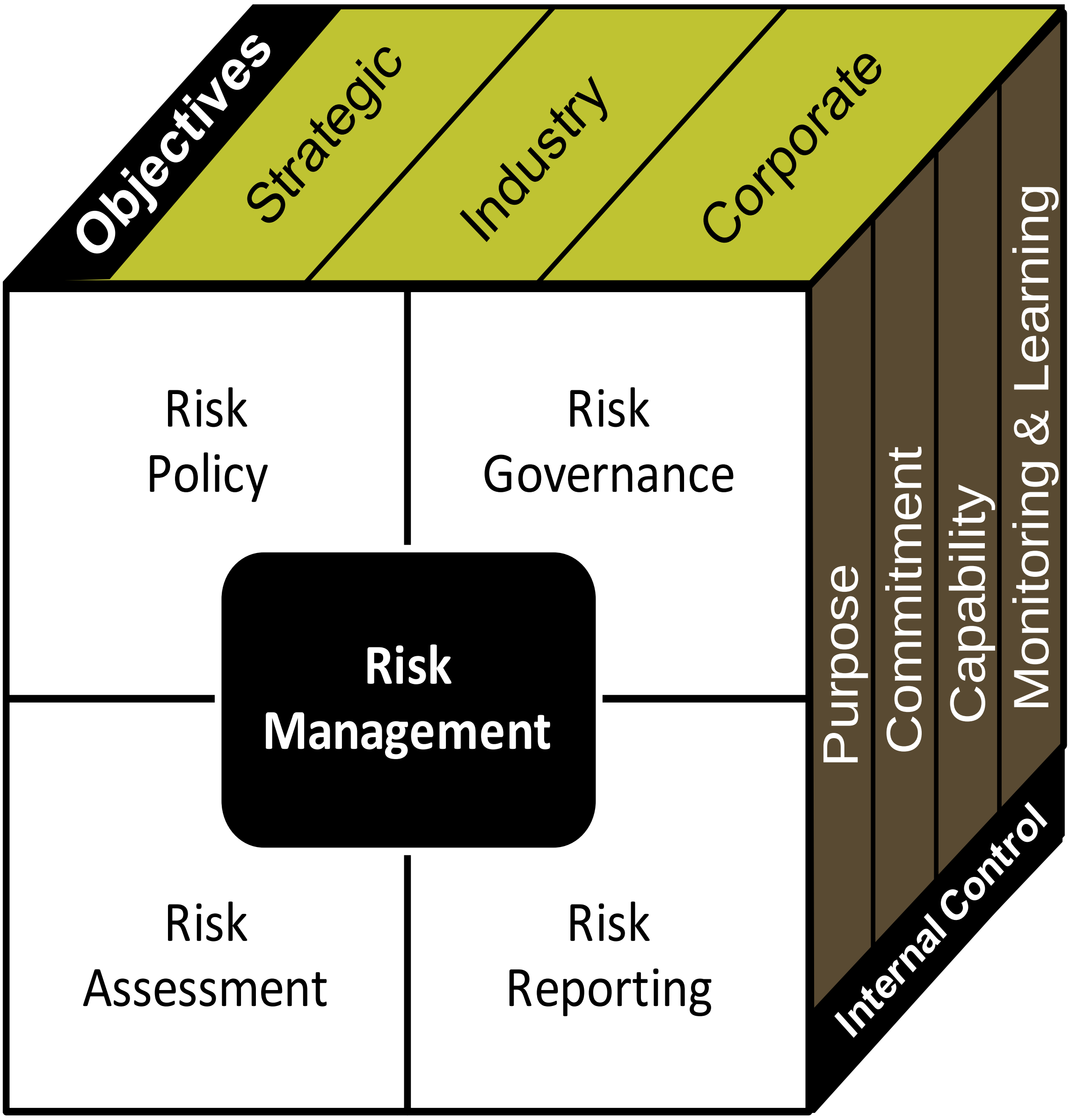
Appendix A - Risk Report Template

Objective:					
Risk	**Previous Risk Level**	**Current Risk Level**	**Risk Level Trend**	**Overall Control**	**Issues**
1.	Very High	Very High		G	• •
2.	Medium	Medium		G	• •
3.	Medium	Medium		A	• •
4.	High	Medium		A	• •
5.	High	High		G	• •
6.	High	Very High		R	• •
7.	Low	Low		A	• •
8.	High	High		A	• •
9.	High	Medium		G	• •
10.	Medium	Medium		G	• •

Assessment reference

Control Indicator	
R	Indicates that risk control actions are not progressing and that management action will be required to bring the situation under control
A	Indicates that most risk control action is being implemented however may be behind schedule or encountering difficulties with implementation. No management action is required now. Future action may be required if the situation persists.
G	Indicates that the risk control action is progressing well. No management action is required.
↑/→/↓	Trend of the risk level is rising/falling/holding

Enterprise Risk Management Framework



COMPONENTS of the ERM Framework

There are three components of the ERM framework:

a. **Objectives** – *identifies the main categories of objectives within the organisation*

b. **Internal Control** – *establishes the factors contributing to effective control of the organisation's internal working environment*

c. **Risk Management –** *defines the policy, governance and methodology for risk management within the organisation*