****

Risk Management Framework

[Purpose 3](#_Toc38981675)

[Scope 3](#_Toc38981676)

[Risk Management Policy 3](#_Toc38981677)

[Introduction 3](#_Toc38981678)

[Context – Why Managing Risk is Important 3](#_Toc38981679)

[Policy Statement 4](#_Toc38981680)

[Roles and Responsibilities 5](#_Toc38981681)

[Risk Appetite Statement 8](#_Toc38981682)

[Risk Management Guideline 9](#_Toc38981683)

[Introduction 9](#_Toc38981684)

[Decisions 10](#_Toc38981685)

[Knowledge 10](#_Toc38981686)

[Support 13](#_Toc38981687)

[Culture 15](#_Toc38981688)

[Communication and Consultation 15](#_Toc38981689)

[Evaluation and Improvement 16](#_Toc38981690)

[Risk Management Procedure 16](#_Toc38981691)

[Definitions 16](#_Toc38981692)

[Risk Management Process 18](#_Toc38981693)

[Establish Context 19](#_Toc38981694)

[Risk Assessment 19](#_Toc38981695)

[Risk analysis 21](#_Toc38981696)

[Risk Treatment 21](#_Toc38981697)

[Monitoring and Review 21](#_Toc38981698)

[Recording and Reporting 22](#_Toc38981699)

# Purpose

The objective of the Risk Management Framework (RMF) is to ensure a consistent approach to the management of all risks across OrgName to ensure risk becomes an integral part of decision making.

The RMF is made up of the Risk Management Policy, Risk Appetite Statement, Risk Management Guidelines and Risk Management Procedure.

# Scope

The RMF applies to all staff, contractors and volunteers and is designed to align and/or link to the frameworks of key stakeholders such as customers and suppliers.

As managing risk is everyone’s responsibility, these guidelines cover all of our organisation as well as our key stakeholders including our customers and suppliers.

# Risk Management Policy

## Introduction

At its core, the aim of a formal risk management framework is to assist the organisation to create and protect value. In our organisation, creating value means …

Risk Management helps in creating value by providing new insights for decision makers about the internal and external environments in which we operate. And protecting that value follows from putting in place processes and systems that help decision makers to recognise the uncertainties they face and to make good, considered, risk-based decisions. Decisions that balance risk and reward.

This policy sets our appetite for risk and our overall approach to managing the inherent uncertainty we face in fulfilling our organisational purpose. It also sets out the legal and regulatory context for our management of risk and our appetite for risk and approach to meeting those obligations.

This policy should be read in conjunction with our Risk Management Guideline which provides detail on the structure, processes and systems we utilise to manage risk. The Guideline also calls up the main Risk Management Procedure that staff will need to utilise to meet the intent of this policy.

## Context – Why Managing Risk is Important

This section establishes the key uncertainties for our decision making due to our inherent internal and external environments and any legal or regulatory requirements for the management of risk. This section is best completed having completed the following analysis tools which are available from the [Learning Resources](https://www.bryanwhitefield.com.au/freebies/) section of my website:

Stakeholder – This tool requires you to list your stakeholders and consider their views on your organisation as well as your strengths and weaknesses in managing their expectations.

Capability – This is a tool to self-assess your organisation’s capability to manage risk.

PESTLE – This looks at your external environment and helps to identify emerging issues

Whilst we have been managing risk since the organisation was formed, society has evolved new expectations for all organisations to manage risk. In order to manage risk effectively we need to consider our internal and external operating environment.

The following paragraph is written for a small organisation and should be adjusted/replaced for larger organisations.

In respect of our internal operating environment, we are a relatively small organisation of less than 200 people. However, we still have the inherent challenge of ensuring the best available information flows to decision makers in a timely manner. Like most organisations we have multiple business units and functions and a range of senior executive positions. This creates silos which are good for focusing on the job at hand. However, silos can also create artificial barriers to communication flow.

The following paragraph is written for a particular type of organisation as an example and should be adjusted/replaced for your organisation.

Our external environment presents us with a range of opportunities and threats. The shift in societal expectations around the provenance of products is to our advantage. However, the fast-changing technology landscape means we face significant challenges in implementing our technology roadmap. Both in meeting our stakeholder’s expectations and in maintaining a suitable cost base.

In terms of our legal and regulatory framework there is no specific requirement to manage risk, however, every organisation has an obligation under the Corporations Act to manage the organisation in the best interests of its stakeholders. This includes, managing risks that are foreseeable.

Given the rise in expectations and the ever-changing business environment, our organisation will benefit from a more formal approach to risk management.

## Policy Statement

Risk management is an essential element of good governance. We are committed to operating a risk management framework that supports decision makers to work towards fulfilling our goals while operating within our appetite for risk as approved by the board. This in turn will deliver value to our stakeholders and build their confidence and trust in us.

Our approach to risk management is aligned with the Australian and international guidance standard AS ISO 31000: 2018 Risk Management – Guidelines. We are committed to adhering to the key principles espoused in the standard (See **Figure 1**) including:

(identify the core principles that align most closely with your core values)

* Operating our framework in the pursuit of the creation and protection of value
* Ensuring that risk is everyone’s business by making it inclusive
* Ensuring information flows efficiently and effectively across silos to decision makers
* Having a flexible framework to cater for the different needs of our business units, and
* Having a framework suitable for our broad cultural mix of staff.

We are also committed to continuing our focus on innovation and creativity as these are critical to our success. While our framework aims to ensure we have an appropriate system of controls to ensure we operate within our appetite for risk, it is also designed to help ensure we are able to be creative and innovative in the design and implementation of our control environment.

With the fast pace of change we operate in, our framework will also be dynamic so that it is designed for continual improvement and so that risk is integrated into our everyday practices as much as is practical to do so.



**Figure 1 – Principles of Risk Management AS ISO 31000: 2018**

## Roles and Responsibilities

The **Board** has ultimate accountability for our organisation. However, day-to-day management is the responsibility of the **Chief Executive** and the members of the **Executive**, inclusive of managing risk. They in turn delegate responsibility to members of their team. Hence, every staff member has some level of responsibility for managing risk.

Our governance structure recognises the shared responsibility to manage risk and consequently we have **board and management committees** in key areas of risk to support decision makers. Our core committees are (list your core committees) (Refer **Figure 2**)

The **Audit and Risk Committee** (ARC) (change to name of your committee) oversees our risk management framework and is responsible for coordinating our management of risk across our governance committees and all other areas of risk. The ARC comprises of (list your committee members by role).

The **Enterprise Risk Management Committee** (ERMC), made up of several senior executives and chaired by the **Chief Risk Officer**, is responsible for the active management of risk by management and staff. Its role is to ensure risks are identified, assessed and effectively managed in accordance with this policy. The ERMC reports quarterly to the ARC.

The ERMC may establish working groups to develop strategies for the management of enterprise-wide risks, such as cyber risk, business continuity and pandemic planning. The ERMC retains oversight of these working groups and facilitates appropriate coordination across the organisation.

The Chief Risk Officer heads the **Risk Team**. The **Risk Team** is an enabling function and is responsible for designing and maintaining the Risk Management Framework. The **Risk Team** do not own the risk of the business. Their role is to partner with the business to support decision makers. To that end, the risk function is responsible for ensuring the Risk Management Procedure, as implemented across the business, is fit-for-purpose, is appropriately resourced and that staff have been trained. Most importantly, the procedure as implemented must provide insight to decision makers about the risks they need to manage and the effectiveness of the controls they have in place.

[If you use risk champions or have a risk community of practice, include them here and describe their role. Also describe in the paragraph above how the Risk Team are responsible for maintaining Risk Champions or a Risk Community of Practice]

**Management** in each area of our business remains responsible for the outcomes of their business, including the management of risks, controls and ongoing monitoring processes. Material risks identified by one area which may have implications for other areas of the organisation should be reported immediately to the relevant area(s) and to Risk and Compliance for coordination.

Incidents that have, could have or may yet cause material undesirable consequences for the business must be reported promptly to Risk and Compliance. In addition, areas are encouraged to report to Risk and Compliance ‘near misses’ that might assist in identifying, evaluating or treating risks.

All **employees** are responsible for managing risk in accordance with this policy, the guidelines and the procedure. Employees are also responsible for reporting identified risks or incidents that they become aware of in the course of their work.

**Internal Audit** (Audit) are responsible for providing assurance to the Executive and the Board that risk is being managed in accordance with this policy. This includes reviewing the organisation's risk management framework and the operation of Risk Management Procedure. This is completed through a program of risk-based audits which include testing controls on a sample basis.

Audit reports independently to the Board's Audit and Risk Committee. Copies of these reports are also made available to the ERMC.

*Red arrows
signify information exchange across silos*

Business Units

Major Incidents

Business Performance and Risk Reporting

Major Risks

Risk Profiles

Workforce Committee

Production Committee

Program Mgmt. Committee

Technology Committee

Enterprise Risk Committee

Board

Remuneration Committee

Quality Committee

Investments Committee

Audit and Risk Committee

Crisis Mgmt. Committee

Major Incidents

Red arrows signify information exchange across silos

Executive

Crisis Mgmt. Committee

Temporary Committees

**Figure 2 – Chart of Information Flow based on Roles and Responsibilities**

# Risk Appetite Statement

For smaller organisations a one-page written Risk Appetite Statement (RAS) maybe sufficient. For larger organisations, the RAS may be a separate document or even a separate framework called up by this policy. Below is an example of referencing/linking to a separate RAS, followed by an example written summary for an organisation seeking only a written statement.

Example for organisation with separate RAS

Orgname must be, and be known to be, insert short summary statement of mission/vision or similar. Our strategy and core objectives to deliver on our mission/vision are outlined in stratplan and dates.

In order to fulfil our mission/vision we must take risk. However, we must take risk within certain boundaries. The type and amount of risk we are willing to take is documented in our Risk Appetite Statement (link).

Sample one-page RAS

Orgname must be, and be known to be, insert short summary statement of mission/vision or similar. Our strategy and core objectives to deliver on our mission/vision are outlined in stratplan and dates.

In order to fulfil our mission/vision we must take risk. However, we must take risk within certain boundaries. An essential part of our “DNA” is for the customer to be at the centre of everything we say and do. This means, we must put the customer before financial gain. Where we can’t meet customer expectations with commensurate financial returns, we will not operate in this area of business. However, for areas of uncertain financial returns, we are willing to take risk, to expend capital, to provide management the opportunity to identify how areas of business can be made profitable while serving our customers as they expect to be served.

The amount of financial risk we are willing to take in determining areas of business to operate in or withdraw from are determined by our financial delegations. These delegations also determine our willingness to take financial risk in growing existing profitable business.

Central to our ongoing success is our reputation with …, Government and the community at large. To ensure the maintenance of our reputation and our “public licence to operate”, we will continue to provide high quality …, in line with our strategic goals and in accordance with our regulatory responsibilities.

In providing the type of services we provide, our staff are sometimes at risk. However, we manage that risk by … supported by fit-for-purpose safety programs and adequately trained staff. We continually reinforce a zero tolerance for serious breaches of our safety procedures and have ongoing efforts to decrease injuries and targets set to monitor reduction. We believe this approach reduces the risk of major (life altering) injury to the lowest possible levels whilst maintaining our commitment to ...

OrgName’s approach to risk reflects the Australian Standard, AS ISO 31000-2018. Consequently, the Executive Team is tasked with embedding our appetite for risk into business-as-usual for all staff. This is accomplished via review of organisational policies, frameworks, processes and systems to ensure they reflect our agreed appetite for risk.

As risk appetite is affected by our internal and external environment, the Board will review this risk appetite statement at least annually and also after any major change to the internal or external operating environments.

# Risk Management Guideline

The guideline establishes for the reader all the different components that are required to be coordinated to manage risk. It provides links up and down the supply chain and across the different business units of an organisation. It also links specific types of risk to the overall approach. For example: safety, environment, cyber etc.

Think of it like a roadmap showing all the main features of managing risk for your organisation and all the roads, trails, rivers and streams connecting them.

## Introduction

The purpose of this Risk Management Guideline is to establish a consistent approach to managing risk across orgname. It provides a roadmap for implementation of our Risk Management Policy endorsed by the … And it guides staff on the key corporate management frameworks and procedures needed for the management of risk.

There are four core elements of the guideline, Decisions, Knowledge, Support and Culture that are underpinned through sound Communication and Consultation and appropriate Evaluation and Improvement of the Risk Management Framework on an annual basis (see **Figure 3**). Each have a separate section in this guideline.

Risk Management Policy - Direction

Risk Appetite Statement - Boundaries

Risk Management Guideline - Roadmap



* Information
* Systems
* Reporting
* Strategies/ Plans
* Programs/ Projects
* Operations/ Processes



Communication and
Consultation

Evaluation and
Improvement

Risk Management Procedure - Processes

## Knowledge

Managing risk means making decisions based on the best information available. This means the communication of information up and down the organisational hierarchy and across silos. **Figure 2** in the Risk Management Policy shows the governance structure for the flow of performance and risk information.

**Figure 4** shows the importance of the organisation’s Risk Appetite Statement (RAS) for decision making and reporting on risk. Including Key Risk Indicators (KRIs) which identify if the business is operating within the tolerances defined by the RAS.

[N.B. For smaller organisations, KRIs may be more effort than the value they bring. Larger organisations need more early warning signs than smaller ones due to the complexity of the organisation and the number of silos]

It also shows how the Risk Team and Internal Audit support the organisation as partners to the business, Executive and the Board (see next section on Support).

Lastly, it shows how the organisation’s approach to managing risk is built on the foundations set by the culture of the organisation (see section on Culture).



**Figure 4: Knowledge Sharing**

Key Risks

Key Risks

The following knowledge management processes and systems are in place to support risk-based decision making.

[modify this list to suit your organisation]

* Enterprise Performance Dashboard - [describe the system utilised for performance reporting using KPIs and KRIs. Instructions to use the system should be in the Risk Management Procedure section. If spreadsheets are used, explain this instead and identify how and where they are stored.]
* Management Information Systems - [describe the risk system utilised and how it is utilised to facilitate the flow of performance and risk information across the organisation and how risk is aggregated at each level of the organisation. Instructions to use the system should be in the Risk Management Procedure section. If spreadsheets are used, explain this instead and identify how and where they are stored. A template should be included in the Risk Management Procedure section. If you wish to move away from spreadsheets, please contact me for my recommendation on systems and on issues to address if building a system internally]
* Record Keeping - [describe your record keeping system for risk information]

## Decisions

Risk management supports decision making. Decisions by default are always made under a degree of uncertainty, otherwise a decision would not be required. While all our decisions should consider risk, some decisions need to document how risk was considered. As a guide, the following is required to fulfil the intent of the Risk Management Policy.

**Board**

For material decisions brought to the Board, the minutes should note the extent risk was appropriately considered in the board paper and any action taken accordingly by the Board.

Material decisions are defined as … and includes strategic plans, business plans/budgets and business cases as examples.

**Executive**

The Executive should ensure the consideration of risk is integrated into:

* Strategic and Business Planning
* Board papers covering material decisions
* Corporate Performance Reporting including at Division and Business Unit level.
* Business Cases

Integrating risk into these processes means that risk is considered as part of the process and reported with normal business reporting.

As a minimum, as part of the annual business planning process, Division and Business Unit managers are required to submit risk profiles with their business plans. The intention is to communicate to the Executive and Board the risks and opportunities around the business plan.

**Portfolio/Program/Projects**

Management should ensure consideration of risk is integrated into portfolio/program/project management and performance reporting. Any project with a value in excess of $100,000, or any project not included in the budget requiring expenditure in excess of $50,000 should have a risk assessment conducted.

**Operations**

Management should ensure management of risk is considered in all areas of operations. This means that the frameworks that support these functions include the consideration of risk in decision making and performance reporting. They include: (list the key functional areas of concern for your organisation):

|  |  |
| --- | --- |
| * Business Continuity
 | * Information Technology
 |
| * Compliance
 | * Investment
 |
| * Contract Management
 | * People and Culture
 |
| * Crisis Management
 | * Procurement
 |
| * Customer Service
 | * Quality
 |
| * Cyber Security
 | * Regulatory Compliance
 |
| * Environment
 | * Safety
 |
| * Facilities Management
 | * Security
 |
| * Finance
 | * Supply Chain
 |
|  |  |

As a minimum, these framework’s corporate policies should be consistent with the Risk Management Policy and the framework guidelines should articulate when a risk assessment is mandatory. They should also ensure the risk assessment methodology used is aligned with the OrgName Risk Assessment Procedure. The requirement for mandatory risk assessments should be based on consideration of OrgName Risk Criteria as outlined in the Risk Management Procedure.

Embedding risk-based decision making as part of Business-As-Usual (BAU) needs to be led top down, however, all staff are responsible for managing risk. Management and staff are set performance expectations through our Performance Management Policy. In addition, the charters of our Board and management committees have clear performance guidelines for the management and oversight of risk.

## Support

Management and staff have obligations as defined in the Risk Management Policy. They are supported across the organisation by the Risk Team. The Risk Team consists of … [describe your team. If you use risk champions, include them and describe their role in the following section]. The team provides support as follows:

The Risk Team is not responsible for the risks managed across the business. They are responsible for providing clear and timely advice. And, when needed, insightful advice into the risks and opportunities facing the business. The following is a guide of how the support the Risk Team will provide:

|  |  |
| --- | --- |
| Role/Area/Function | Support Provided |
| Board | Facilitate Board discussions/assessments of risk as required.Provision of expert opinion on risk issues as required.  |
| Executive | Facilitate enterprise-wide risk assessment to support the Executive in reporting on strategic risk when performance reporting to the Board. |
| Portfolio/Program/Projects | Work with managers [and their risk champions/risk coordinators if following that model] to ensure risk management programs adequately assist management and staff fulfil their obligations under the Risk Management Policy.Provide advice on how to conduct risk assessments and to facilitate risk workshops on request.Assist in building risk management capability within the business. |
| Operations | Work with support function framework owners (Safety, Environment …) [and their risk champions/risk coordinators if following that model] to ensure each framework assists management and staff fulfil their obligations under the Risk Management Policy.Provide advice on how to conduct risk assessments and to facilitate risk workshops on request.Assist in building risk management capability within the business. |
| Risk Champions [if using this model] | Develop and maintain a Risk Community of Practice for the sharing of information and for input into design and maintenance of the Risk Management Framework  |
| Staff | Develop appropriate online and in-person training so that staff at all levels and in all areas of the business have sufficient skills to fulfil their responsibilities as outlined in the Risk Management Policy. |
| Internal Audit | Collaborate to assist in identifying the key risks and key controls that are to be assessed through the Audit Plan each year.  |

## Culture

Our culture needs to reflect our attitude to risk taking which should reflect in the behaviours we see from all staff.

Describe the culture you seek. For example:

Our core values ask us to have a passion for delivering best results, to operate with trust and integrity, to innovate and collaborate and to be inspirational in our leadership. Managing risk is integral to living these values.

For example, *best results* flow from anticipating potential obstacles to our success and putting in place plans to address them. *Trust and integrity* are strengthened by delivering on what we say we will do and avoiding behaviours that lead to fraud and corruption. Risk management can also drive our *innovation* agenda. Often, the highest risks we face are in most need of innovation. And they are best addressed through *collaboration*.

And finally, part of *inspirational leadership* comes from taking calculated risk.

Our values guide the risk-taking behaviours we wish to see.

## Communication and Consultation

All staff are required to fulfil their roles and responsibilities defined by the Risk Management Policy. Staff at all levels need to be aware of this and need support through appropriate levels of communication and consultation. This is facilitated through:

[describe your approach. Examples below]

* **Training:** Stakeholders need sufficient understanding of risk and the risk management process to manage the risk to achieving their goals. Therefore we provide a range of training to staff, including and initial introduction to risk and our risk management framework through the induction process.
* **Communication:** Stakeholders need to be aware of risks to manage them. Awareness is created through our knowledge management systems, however, the way risk is communicated is important. Our approach is to minimise the use of risk management jargon and to use common business language.
* **Consultation:** Stakeholders, internal and external, need to be consulted for a range of reasons. These include to promote and confirm awareness of risk, clarify ownership of risk, bring different expertise together to manage risk and to facilitate a common understanding of our appetite for risk as an organisation.
* **Incident Management and Lessons Learned:** We foster a culture of open and honest communication about risk. This means we promote the early reporting of incidents, including near misses. They are handled through our Incident Management System which has a built-in workflow for escalation of individual risks and for analysing and reporting on systemic risks. Systemic risk is where multiple incidents of a similar nature are occurring due to a common cause. The common cause is not always evident without analysis. For example, high levels of sick leave may identify a culture of bullying.
* **Whistleblowing:** Our Whistleblowing Policy encourages employees to raise concerns they might find difficult to raise with their manager by providing them access to an independent body with guaranteed confidentiality.

## Evaluation and Improvement

The effectiveness of the Risk Management Framework is evaluated annually through independent assessment of the organisation’s performance against the four core elements of this Risk Management Guideline, Decisions, Knowledge, Support and Culture. The independent assessment consists of:

* Decisions – The degree to which risk was considered in key decisions. Decisions that were considered successful as well as those that were assessed as not.
* Knowledge – The quality and timeliness of the flow of risk information to and from decision makers.
* Support – The quality and timeliness of support provided by the Risk Team.
* Culture – The extent the behaviours of management and staff reflected the culture sought. Initial evidence will be the findings from the review of the other core elements of the guidelines (Decisions, Knowledge and Support) as well as from staff surveys, review of incidents and lessons learned and a review of any reports to the whistle-blower independent body.

Recommendations for improvement will be prepared for consideration by the Audit and Risk Committee which will provide a recommendation to the Board for endorsement.

# Risk Management Procedure

## Definitions

**Acceptable level of risk**

The acceptable level of risk reflects the decision by management to accept the likelihood and consequences of a risk.

**Consequence**

The outcomes associated with a risk occurring e.g. the loss, injury, disadvantage or gain.

**Control**

An existing process, policy, device, practice or other action that acts to minimise negative risk or enhance positive opportunities.

**Likelihood**

Likelihood is the qualitative description of the probability or frequency of a risk occurring.

**Risk**

Risk is the effect of uncertainty on objectives. Risk in OrgName is expressed in terms of the sources of risk, the potential consequences and the combined level of likelihood from all sources of risk.

**Risk Analysis**

The systematic process to understand the nature of and to deduce the level of risk

**Risk Assessment**

Risk assessment is the overall process of identifying, analysing and evaluating risk.

**Risk Evaluation**

The process of comparing the level of risk against risk criteria.

**Risk Identification**

Risk identification is the process of determining what can happen, where, when, why and how.

**Risk Management**

The coordinated activities to direct and control an organisation with regard to risk.

**Risk Management Process**

The systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk

**Risk Profile**

The risk assessment output document prepared by each business unit which contains all the risks identified and the assessment of those risks.

**Risk Retention**

Acceptance of the burden of loss, or benefit of gain, from a particular risk.

**Risk Sharing**

Sharing with another party the burden of loss or benefit of gain from a particular risk.

**Risk Treatment**

The process of selection and implementation of measures to modify risk

**Stakeholders**

Stakeholders are those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity of OrgName

## Risk Management Process

This risk management process we follow is as outlined in the Australian and international standard on risk management, AS ISO 31000:2018 Risk Management. The core process is shown here. The same process is applicable for strategic, operational and compliance related activities. Each of the elements of the process are explained below.

Insert your version of the risk process that is suitable for your organisation.



**Figure 1: The Risk Management Process**

**Source: AS ISO 31000: 2018**

### Establish Context

The purpose of this step is to define the basic parameters within which risks must be managed and sets the scope for the rest of the risk management process. This involves understanding the internal and external environment in which risks may occur including strategic, operational, financial, stakeholder, social, cultural and legal aspects of your functions. This will provide the structure for the risk assessment tasks that follow.

The criteria for assessing the level of risk has been established at the organisation level via the OrgName Risk Criteria and Risk Matrix template.

Tools and templates to assist in establishing context are available here. Link to tools such as Stakeholder, PESTLE, Capability and Value Chain analyses and others your organisation uses.

### Risk Assessment

#### Identifying, analysing and evaluating risk

1. **Identify** the sources of risk, areas of impacts and whether the source is within our control.
2. **Analyse** the causes of risk, the consequences and existing controls in place to modify the risk.
3. **Evaluate** by using the results of the analysis to make decisions about OrgName’s appetite for the risk and whether additional actions are needed to reduce the risk’s likelihood or impact.

The approved OrgName Risk Template for recording the risk assessment is attached to this procedure.

N.B. Business Unit and Project risk assessments should not be conducted by individuals, they should be conducted in small teams and can be facilitated by managers or other staff as available. External assistance can also be sought for facilitation. For larger or more complex risk assessments, you are encouraged to involve a broad cross-section of staff and include staff not specifically involved in the area of business/project to further stimulate thinking around risks and opportunities.

###### Identifying Risks

We identify risks by generating a comprehensive list of threats and opportunities based on events that might affect the achievement of priorities.

To identify risks, undertake a comprehensive scan of our operating environment, identify the sources of risks and assess how risks affect the achievement of priorities.

**Information sources and methods to identify and assess risks**

Examples of information sources and methods to identify, analyse and evaluate risks include:

| Source | Description | Source | Description |
| --- | --- | --- | --- |
| Corporate history | Individuals’ experiences and records to understand what happened in the past | **Stakeholder analysis** | Considers risks from stakeholders’ perspectives |
| Interviews | Data collection with individuals and/or focus groups and gathering local intelligence | **Process analysis** | Analyse processes to identify opportunities to improve |
| Surveys/ questionnaires | Data from internal and external customers and stakeholders | **Other organisations** | Similar experiences and knowledge |
| Environmental analysis | PESTLE: Political, Economic, Sociological, Technological, Legal, EnvironmentalSWOT: Strengths, Weaknesses, Opportunities, Threats | **Scenario planning** | Possible (often extreme) future states to anticipate how threats and opportunities might develop |
| Planning – strategic and operational | Monitoring of risk while reviewing performance against objectives, performance indicators and expected outcomes | **Existing risk registers** | Risks, risk levels, controls and actions |

**Writing a risk description**

A good risk description will:

be clear and written in plain English (no acronyms)

define the risk story in a way that is easy for anyone in to understand

promote a common understanding of the risk

explain the main source(s) and main effect(s) of the event

inform the design of appropriate controls and actions to mitigate the risk.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Ask: |  | Example of a poor description |  | Example of a good description |
|  | What is the event that could happen? |  | *There is a risk to services* |  | *There is a risk that services will not be provided* |
|  |  |  |  |  |  |
|  | What is the trigger or source of the risk?  |  | *because of funding* |  | *caused by a reduction in program funding*  |
|  |  |  |  |  |  |
|  | What is the main consequence of the risk occurring on achieving objectives? |  | *leading to a reduction in services.* |  | *resulting in an inability to achieve program objectives.* |

### Risk analysis

Risk assessment helps us to understand our risk profile and the effectiveness of the controls and actions used to manage and mitigate risks. We assess risks at two points:

**current risk level** takes into account the controls that exist and assesses the risk level with those controls in place

**target risk level** isthe risk level you are aiming for after considering OrgName’s risk appetite and recognising that some level of risk is both manageable and unavoidable.

The risk level is determined by assessing the consequence and the likelihood of the risk occurring. We do this by using the OrgName Risk Criteria and Risk Matrix (attached to this procedure) to combine likelihood and consequence.

### Risk Treatment

If the current risk level is undesirable, measure for managing the risk should be devised and implemented. Once implemented they become existing controls unless they are temporary measures.

Or in the course of the risk assessment additional measures are identified to manage risk more effectively, these also become risk treatments and are recorded in the risk assessment.

### Monitoring and Review

Monitoring of risk entails monitoring the underlying assumptions on which the risk assessment was based and monitoring the effectiveness of controls.

Controls are internal controls put into place to manage material risks to the business. Examples include procurement processes, administration policies and procedures, recruitment processes and codes of conduct. Management is responsible for the design, implementation and maintenance of internal controls. In order to maintain controls, management should devise an appropriate testing regime to identify any weaknesses in the control environment.

Internal Audit is responsible for ensuring appropriate assurance processes are in place to provide assurance to the Board the internal control framework is appropriate for the business and is effective.

### Recording and Reporting

Recording of the risk assessment is to be completed using the OrgName Risk Template (attached to this procedure). Reporting lines are as per the Risk Management Policy and the timelines for reporting are shown in Table ?.

Table ? – Timelines for reporting and monitoring and review of risk assessments

|  |  |  |  |
| --- | --- | --- | --- |
| **Current****risk level** | **Treat** | **Report** | **Review** |
| **Extreme** | As soon as possible | Monthly risk updates to governing body or management team and risk stakeholders | Monthly review by risk owner until effectively mitigated, including risk action updates |
| **High** | As soon as practical | Monthly risk updates to governing body or management team and risk stakeholders | Monthly review by risk owner until risk is effectively mitigated, including risk action updates |
| **Medium** | Within three (3) months evaluate effectiveness of controls and actions applied to the risk | As required provide risk update to governing body or management team and risk stakeholders | Quarterly review by risk owner including risk action update (if applicable) |
| **Low** | Maintain effectiveness of current controls and manage by routine procedures | As required provide risk update to governing body or management team and risk stakeholders | Monitoring and review schedule should be considered based on potential rapid escalation / volatility of the risk |



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk** | **1.0** |  | **Impact of risk happening** | **Consequence** | **Likelihood** | **Risk Level** |
|  Describe the risk to an objective in a sentence here |  List impacts and quantify as much as possible | Ratings from Risk Criteria | Ratings from Risk Criteria | Ratings from Risk Criteria |
| **Risk Owner** | Position most responsible for the outcomes of this objective  | **Review Date, Trend and Target Risk Level** |  |  |  |
| **Source No.** | **Sources** | **Current controls and adequacy of controls** | **Risk Treatments** | **Person Responsible** | **By When** | **Trend** |
| **A = Fully Adeq. M = Moderately Adeq. I = Inadequate** |
| **1.1** | Describe different reasons why this risk/opportunity may or may not eventuate | Describe what we are CURRENTLY doing to manage this | Control Rating? | Describe what we are going to do in the future |   | Must be a definitive date |   |
| **1.2** |   |   |   |   |   |   |   |
| **1.3** |   |   |   |   |   |   |   |
| **1.4** |   |   |   |   |   |   |   |
| **1.5** |   |   |   |   |   |   |   |
| **1.6** |   |   |   |   |   |   |   |

####