matamata piako district council






Risk Management Framework

Document History

VERSION	DATE	REVISION DETAILS	AUTHOR	APPROVED
1.0		New Version	I. Galymzhan	

Content

1. Introduction

Matamata-Piako District Council (MPDC) acknowledges that it exists to provide value for diverse groups of public and private external stakeholders. We face myriad number of risks that affect our ability to achieve strategy and business objectives underpinning our vision to make Matamata-Piako 'The Place of Choice'.

The management of risk is an essential component of performance management and represents good governance. If we are to make sustained improvement risk management must be embedded throughout the organisation. We need to be realistic and open about the risks that we face and ensure that risk registers are updated and used for real-time management purposes. We recognise the importance of risk management and are actively reviewing and monitoring the key risks that we face.

Formally incorporating risk management into day-to-day management (strategy setting and performance processes) increases the focus on what needs to be done (and not done) to meet strategy and business objectives.

Through the implementation of an integrated and consistent approach to risk management, we aim to achieve the following risk management objectives:

- An organisational culture of reliable, informed, evidence based planning and decision making;
- A consistent approach to the identification, assessment and treatment of risks;
- Improved communication on matters of risk to enhance decision making;
- Proactive and adaptive management practices;
- Support achievement of our strategy and business objectives;
- Effective allocation and use of resources for risk treatment;
- Enhanced identification of opportunities and threats;
- Reduced performance variability;
- Enhanced organisational resilience and continuity of service;
- Improved operational effectiveness and efficiency;
- Employees accountability for risk identification and treatment;
- Improved corporate governance, controls and performance;
- Improved community confidence and trust by providing assurance that risks are appropriately managed;
- Reduced liability exposure and financial loss;
- Safeguarding our resources – people, finance, property and reputation.

These objectives will be achieved by:

- Establishing clear roles, responsibilities and reporting lines in our organisation for risk management – making clear that everyone should take ownership for risk management;
- Incorporating risk management considerations into all levels of business planning and service delivery;
- Providing opportunities for shared learning on risk management across our organisation;
- Offering a framework for allocating resources to identified priority risk areas;
- Reinforcing the importance of effective risk management as part of the everyday work of employees by offering training;
- Providing easily accessible procedures, tools and guidance for employees to adequately identify, document, understand and manage risks;
- Building a positive and proactive risk aware culture throughout the organisation.

The risk management framework is aligned to the principles set out in the universally accepted standards: ISO 31000: 2018 Enterprise Risk Management and 2017 COSO ERM – Integrating with Strategy and Performance.

2. Key terms

Business context – the trends, events, relationships and other factors that may influence, clarify, or change our current and future strategy and business objectives.
Business objectives – measurable steps we take to achieve our strategy.
Council – the Mayor and elected Councillors.
Culture – attitudes, behaviours, and understanding about risk, both positive and/or negative that influence the decisions of employees, and reflect our mission, vision, and core values.
External environment - anything outside of our organisation that influences the ability to achieve strategy and business objectives.
Impact – the result or effect of a risk. There may be a range of possible impacts associated with a risk. The impact of a risk may be positive or negative relative to the organisation's strategy or business objectives.
Inherent risk – refers to the initial assessment of the risk prior to considering any of the treatments i.e. the likelihood and impact are assessed without taking into account any mitigation actions (treatments) that currently exist to mitigate the risk.
Internal environment – anything inside of our organisation that influences our ability to achieve strategy and business objectives.
Internal stakeholders – parties working within our organisation such as employees, management, and the Council.
Key risk register - the risk register containing the highest level of risks that may have impact on achievement of the strategy and business objectives.
Key risk indicator (KRI) – indicator providing early warning of risk sources changes in various areas of activity.
Likelihood – the chance of something happening, the estimated likelihood and relative occurrence.
Opportunity - a potential action that may be associated with an existing risk or could result in new risk/s.
Portfolio view – a composite view of risk we face, which positions our organisation to consider the types, severity, and interdependencies of risks and how they may affect our performance relative to our strategy and business objectives.
Promapp - a software application utilised for the quality management system.
Risk capacity – the maximum amount of risk we are able to absorb in pursuit of strategy and business objectives.
Risk owner – the person with the accountability and authority to manage a risk.
Risk profile – a composite view of the risk assumed at a particular level of our organisation or aspect of the business that positions management to consider the types, severity, and interdependencies of risks, and how they may affect performance relative to the strategy and business objectives.
Risk source – a risk source has the intrinsic potential to give rise to risk. A risk source is where a risk originates. It's where it comes from.
Risk register – a document or application containing a record of identified risks with relevant objectives, including risk number, risk statement, risk sources, risk assessment, tolerances and existing controls.
Residual risk – is the actual risk after considering the implemented treatments. The treatments will reduce either the likelihood and/or the impact.
Risk – an uncertain event or condition that, if it occurs, has a positive or negative effect on objectives. It is often expressed in terms of a combination of the impact of an event and the associated likelihood of occurrence.
Risk appetite – the types and amount of risk, on a broad level, we are willing to accept in pursuit of value.
Risk assessment – the overall process of identifying and assessing the impact of risks.
Risk impact category – these are areas in which a risk has impact or consequence to the organisation.

Risk map – a graphic and textual representation of a limited number of our organisations risks arranged as a rectangular table, with the risk's impact (consequence) indicated along one "axis", and the likelihood (probability) or frequency of its realization along the other one.
Severity – a measurement of considerations such as the likelihood (probability or frequency) and impact of events or the time it takes to recover from events.
Controls – any measure or action that modifies or regulates risk. Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk. Risk treatments become controls, or modify existing controls, once they are implemented.
Treatment owner – is the person or persons assigned responsibility for managing, updating and/or monitoring a risk treatment.
Tolerance - the boundaries of acceptable variation in performance related to achieving business objectives.

3. Governance and Culture

The mandate for risk management comes from Council and Executive team (the E-Team). The continued engagement and support of these groups is critically important – without it, risk management fails. These groups understand this and are committed to ensuring sustainable and effective risk management. This commitment must be mirrored by the E-team and the Management group members (the Management) and employees at all levels.

3.1 Risk Roles and Responsibilities.

To ensure the effectiveness of risk management framework (RMF), the Council and the E-team need to rely on adequate monitoring and assurance functions within our organisation. The framework uses the three lines of defence model which is a simple way of explaining the relationship between these functions and acts as a guide to how responsibilities should be divided:

- First line of defence – functions (people, process & technology) that own and manage risk. It is imperative that the Management must understand and accept their accountability for owning and managing their risks.
- Second line of defence – management and oversight; functions that oversee and specialise in risk management and compliance; and
- Third line of defence – internal/external audit; functions that provide independent assurance.

Council	Responsible for overall risk oversight and: • approval of the risk management framework; • approval of key risk register and risk map; • approval of risk treatment plans on key risks; • approval of risk appetite and tolerances.
Audit & Risk Committee	Responsible for: • review of key risk register and risk map • review of key risk indicators; • preliminary approval of risk appetite and tolerances; • review of the effectiveness of the risk management framework; • review of risk treatment plans on key risks; • ensuring that adequate risk management processes have been designed and implemented to manage identified risks.
The Chief Executive Officer (1st line of defence)	Responsible for overall management of risk and: • determination how risk management activities will be coordinated in the organisation; • allocation resources to achieve the objectives of the risk management framework
E-Team members (1st line of defence)	Responsible for undertaking a leadership role for risk management in the organisation and: • Promotion of awareness of the risk culture and risk management in the organisation; • Advising on risk appetite and tolerances; • Regularly monitoring and review of key risk register; • Ensuring compliance with risk management practices and procedures within their respective groups; • Promotion of a learning culture where process or system successes or failures provide an opportunity to improve.

	• Strategic risk identification, assessment and management.
Management Group members (1st line of defence)	Responsible for managing risk in their respective areas of accountability and responsibility and • supporting employees in identifying, managing and communicating risk. • promoting risk management in support of an organisational risk aware culture.
Risk Manager (2nd line of defence)	Responsible for coordination and progression of the organisations risk management methodology and • Administration of risk management framework and implementation of risk training to employees. • Development of a risk improvement plan specifying the proposed risk improvements. • Maintenance of a database of realised risks. • Control over the process of update of risk registers, risk map and risk treatment plans on key risks. • Arrangement and coordination of the process of risk identification and assessment. • Preparation of consolidated reports on risks, and submission of them to the ARC and the Council.
Risk Coordinators (1st line of defence)	Responsible for promoting risk awareness within the business unit at the operational and project level i.e. risk awareness within day to day operations and risk management at the planning phase and during key projects.
All employees (1st line of defence)	Responsible for awareness of risk management processes within organisation and • Everyday identification and management of risks and improvement actions to minimise risk events and impacts. • Identification and management of risks throughout operational and project business (and where appropriate escalation for management and visibility on the key risk register). • Provision of reports on the implementation of risk treatment action plans on key risks to the risk manager. • Provision of timely and complete information on risks (potential/realised) to interested parties, including, but not limited to, provision of information on risks to the risk manager. • Implementation, monitoring and improvement of control procedures within entrusted business processes.
Internal Audit External Audit (3rd line of defence)	Internal audit - contribute to the accuracy and integrity of key risk register (as part of the risk-based approach to audit) with particular regard to the effectiveness of existing controls. External audit – review framework design and implementation.

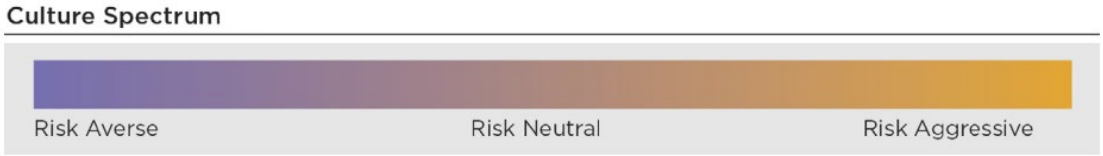
3.2 Culture

The culture, capabilities and practices are integrated into strategy and execution that we rely on to manage risk and in creating, preserving and realising value to our community. Commitment to core values is fundamental to efficient functioning of the RMF.
We must embrace risk-aware culture by:

- *Maintaining strong leadership:* The Council and the Management place importance on creating the right risk awareness and tone throughout our organisation. Culture and, therefore, risk awareness cannot be changed from second-line team or department functions alone;
- *Employing a participative management style:* The Management encourages employees to participate in decision-making and discuss risks to the strategy and business objectives;
- *Enforcing accountability for all actions:* The Management documents policies of accountability and adheres to them, demonstrating to employees that lack of accountability is not tolerated and that practicing accountability is appropriately rewarded;
- *Aligning risk-aware behaviours and decision-making with performance:* Remuneration and incentive programs are aligned to the core values of our organization including expected behaviours, adherence to codes of conduct, and promoting accountability for risk-aware decision-making and judgment;
- *Embedding risk in decision-making:* The Management addresses risk consistently when making key business decisions, which includes discussing and reviewing risk scenarios that can help everyone understand the interrelationship and impacts of risks before finalizing decisions;
- *Having open and honest discussions about risks we face:* The Management does not view risk as being negative, and understands that managing risk is critical to achieving the strategy and business objectives;
- *Encouraging risk awareness across our organisation:* The Management continually sends messages to employees that managing risk is a part of their daily responsibilities, and that it is not only valued but also critical to our success and survival.

The culture affects how risk is identified, assessed and responded to from the moment of setting strategy through to execution and performance given the influence of internal and external factors. We acknowledge that level of the culture may affect:

- Scoping of strategy and business objectives.
  The culture of organisation may affect the types of strategic alternatives being considered.
- The level of rigor applied to the risk identification and assessment processes. *Depending where an organization sits on the culture spectrum, the nature and types of risks and opportunities may differ. What are viewed as potential risks by a risk-averse organisation may be considered as opportunities worthy of pursuit by another.*
- Selecting risk and allocating finite resources.
  A risk-averse organisation may allocate risk treatments or additional resources in order to gain higher confidence of the achievement of a specific business objectives. The cost and benefits associated with incremental risk treatments may be interpreted less favourably by more risk-aggressive organisation.
- The level of reviewing performance.
  Trends in the risk profile or business context may be addressed differently by organisations on different points of the culture spectrum. A risk-averse organisation may make changes more quickly to risk treatments as variations in performance identified. Organisations that are more risk aggressive may wait longer before making changes or may make smaller changes.



We position ourselves on the culture spectrum as risk neutral and it must be reflected in the formulation of risk appetite statement.

4. Integration into organisational processes

Risk management process is an iterative process, which consists of activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, and reporting risk, and must be systematically applied and integrated to our established activities.

Figure 1. Integration into organisational processes

In particular risk management process must be embedded in the following key processes:

Planning and budgeting process: a step in integrating risk management process may simply be to include one page to articulate: first, what events are business units concerned with that may impair their ability to achieve budget/business plan objectives, and second describe what activities they will undertake to monitor and manage those possible events.

Project and programme management: As part of good project management practice, risks are actively identified, managed, escalated and reported throughout the lifetime of the project.

Development and review of our policies and procedures: our policies and procedures specify the approach and expected actions required to manage a variety of risks, including those associated with legislative compliance, people management, finance and asset management.

Procurement and asset management: Risk management must be factored into decision making for significant procurement and asset management related processes.

5. Risk profiling

Assessing risks to the strategy and business objectives requires our organisation to understand the relationship between risk and performance. Risk profile provides a composite view of the risk at particular level of organisation (overall organisation level, business unit level). We should initially understand the potential risk profile when evaluating alternatives strategies. Once strategy is chosen, the focus shifts to understanding the current risk profile for that chosen strategy and related business objectives.

We shall use the below concept in enhancing the conversations of risk, risk appetite, tolerance, and the overall relationship to performance targets. Such a representation considers risk as a continuum of potential outcomes along which we must balance the amount of risk to our desired performance.

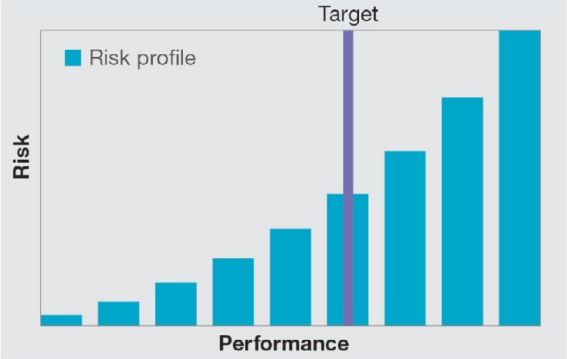


Figure 2. Risk Profile

In figure 1. Each bar represents the aggregate amount of risk for a specific level of performance for a business objective. The target line depicts the level of performance chosen by the organisation as part of strategy-setting, which is communicated through a business objective and target.

Risk profile helps management to determine what amount of risk is acceptable and manageable in the pursuit of strategy and business objectives. Risk profiles may help management:

- Understand the level of performance in the context of the organisation's risk appetite;
- Find the optimal level of performance given the organisation's ability to manage risk;
- Determine the tolerance for variation in performance related to the target;
- Assess the potential impact of risk on predetermined targets.

6. Strategy and Objective setting

6.1 Business context

We consider business context when developing strategy to support mission, vision and values.

We have complex and diverse missions that set the stage for the overall strategy to provide services to the community. Developing and carrying a strategy can be complicated by changes in budget, political climate, highly visible community oversight, and overall mission.

We may be influenced by any or all of the following external factors:

- Political landscapes that affect funding and priorities.
- Budget allocations by legislatures that impact the priorities and any mission changes.
- Demographic, including population growth rates and age distribution that impact the size of the population we serve.
- Technological shifts that impact the type and amount of automation within operations and the challenge to keep pace.
- Changing leadership within government that create new priorities or modify existing ones.
- Climate change, which impacts scrutiny of related government policies.

We may also be influenced by the following internal factors:

- Availability of capital, which depends on the current political atmosphere and may require our organisation to constrain activities or quickly relocate funds.
- Attrition and competition, which can impact the availability of highly skilled employees.
- Operational failures that challenge the ability to carry out mission.
- Availability of investment for technology infrastructure that impacts the ability to perform and interconnected activities.

6.2 Risk Appetite

We define risk appetite in the context of creating, preserving, and realising value. Risk appetite is based on the established prior strategies, mission, vision and culture.

- Risk appetite is the acceptable type and amount of risk for our organisation in course of the achievement of the set strategy and business objectives.
- Risk appetite determines the upper limit of the key risks. It also influences distribution of resources, arrangement of processes, and creation of the organisational infrastructure necessary for efficient monitoring and responding to risks.
- Risk appetite can be either quantitative or qualitative or combination of the both, the best approach is to align with risk assessment criteria.
- Risk appetite (risk appetite statement) is characterised as follows:

    - it reflects our strategy, including business objectives, financial restrictions, and expectations of the stakeholders;
    - it embraces every key aspect (direction) of activity;
    - it considers the desire and the ability to take risks;
    - it defines our attitude towards risk;
    - it is regularly revised with the consideration of business context;
    - it requires efficient monitoring of the risk.

- We shall, no less than once a year, determine the risk appetite, i.e. ability to take risks in order to pursue our strategy and business objectives.
- Risk appetite can be articulated in the context of:
  - Strategic categories;
  - Commonly used objectives;
  - Risk categories.
- Risk profile, risk capacity, RMF capability and maturity may also be considered while determining risk appetite.
- Risk capacity is the maximum amount of risk we can absorb in pursuit of strategy and business objectives.
- To articulate the amount of risk we are willing to take to achieve strategy risk appetite scale may be used to provide a system of gaining uniform consensus across our organisation on the level of risk we are willing to take (see appendix 1. Risk appetite scale).
- Wherever possible, risk appetite statements shall be using language that mimics that used for strategy and business objectives.
- All our risk appetite-related results and suggestions shall be agreed with the business units concerned, including those in charge of the strategy, planning, and corporate financing.
- The obtained risk appetite shall be regarded as a basis of further risk management-related decision-making. To fully embed risk appetite into decision-making at various levels, it needs to be cascaded through and align with other practices.
- Risk appetite is communicated to appropriate levels within our organisation, either broadly or to senior roles only.

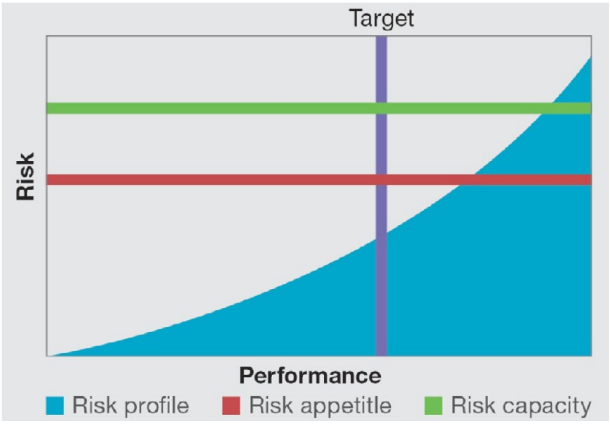


Figure 3. Risk Profile showing Risk Appetite and Risk Capacity

In Figure 2, the risk appetite is plotted as a horizontal line parallel to the x-axis (performance). The gradient of the line indicates that the risk appetite remains constant for all levels of performance at a given point in time. The y-axis (risk) uses the same metric or expression of risk appetite as is referred to in our risk appetite statement.

6.3 Evaluating alternative strategies

We shall evaluate alternative strategies as part of strategy-setting and assess the risk and opportunities of each option. Alternative strategies shall be assessed in the context of our resources and capabilities to create, preserve, and realise value.

- Strategy selection shall include the evaluation of alternative strategies with identification of related risks to each option. Derived risk profile shall assist in choosing the best strategy to adopt given our risk appetite.
- The identified risks collectively form a risk profile for each option of alternative strategies. Determined risk profile allows the Management to consider the types and amount of risk we will face in carrying out the strategy. It will allow the Management to determine what resources will be required and allocated to support carrying out the strategy.
- Alternative strategies should be evaluated using the following approaches: SWOT analysis and scenario analysis.
- We shall hold periodic strategy-setting sessions to outline both short-term and long-term strategies.

6.4 Formulating Business objectives

We develop business objectives that are specific, measurable or observable, attainable, and relevant. Business objectives provide the link to practices within our organisation to support the achievement of the strategy.

- We consider risk while establishing the business objectives at various levels that align and support strategy.
- The goals of our activities are determined at the strategic level, and set the basis for the development of the business objectives.
- Business objectives are aligned with strategy, and cascaded throughout our organisation and our business units.
- Business objectives are to be defined before identification of potential risks capable of negatively affecting the achievement of such objectives.
- Business objectives should align with our risk appetite to ensure that we are not taking too much risk and exceeding our risk appetite.
- We need to have a reasonable expectation that a business objective can be achieved given the risk appetite and resources available to us. Otherwise, we may choose to exceed our risk appetite, procure more resources, or change the business objective.
- Common business objectives are grouped into common categories. Business objectives may be grouped to align with specific aspects of the strategy or with various business groups.
- We set targets to monitor the performance and support the achievement of the business objectives.
- Tolerance – the acceptable variation in performance, it needs to be closely linked to the risk appetite. Tolerance describes the range of acceptable outcomes related to achieving a business objective within the risk appetite. Tolerance shall be developed for each business objective.
- Tolerance provides an approach for measuring whether risks to the achievement of strategy and business objectives are acceptable or unacceptable. Tolerance is tactical and focused; it should be expressed in measurable units, preferably in the same units as the business objectives.
- In setting tolerance, we consider the relative importance of each business objective. The higher is the importance of business objective to the achievement of strategy the lower is the range of tolerance.
- Operating within the defined tolerance provides the Management with greater confidence that we remain within our risk appetite and provide a higher degree of comfort that we will achieve our business objective.

- Performance measure related to business objective enables the confirmation that actual performance is within the established tolerance.
- Tolerance also considers both exceeding and trailing variation (positive or negative).

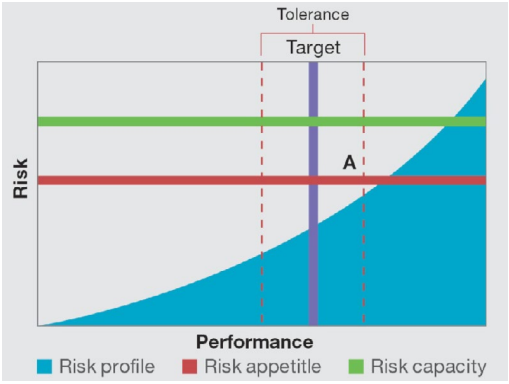


Figure 4. Risk Profile showing tolerance

In figure 3. The right boundary of acceptable variation should generally not exceed the point where the risk profile intersects risk appetite. The maximum point where the performance target could be set is where the right boundary of tolerance intersects with risk appetite.

6.5 Relationship between Risk Appetite and Tolerance

To fully embed risk appetite into decision-making at various levels, it does need to cascade through and align with other practices.

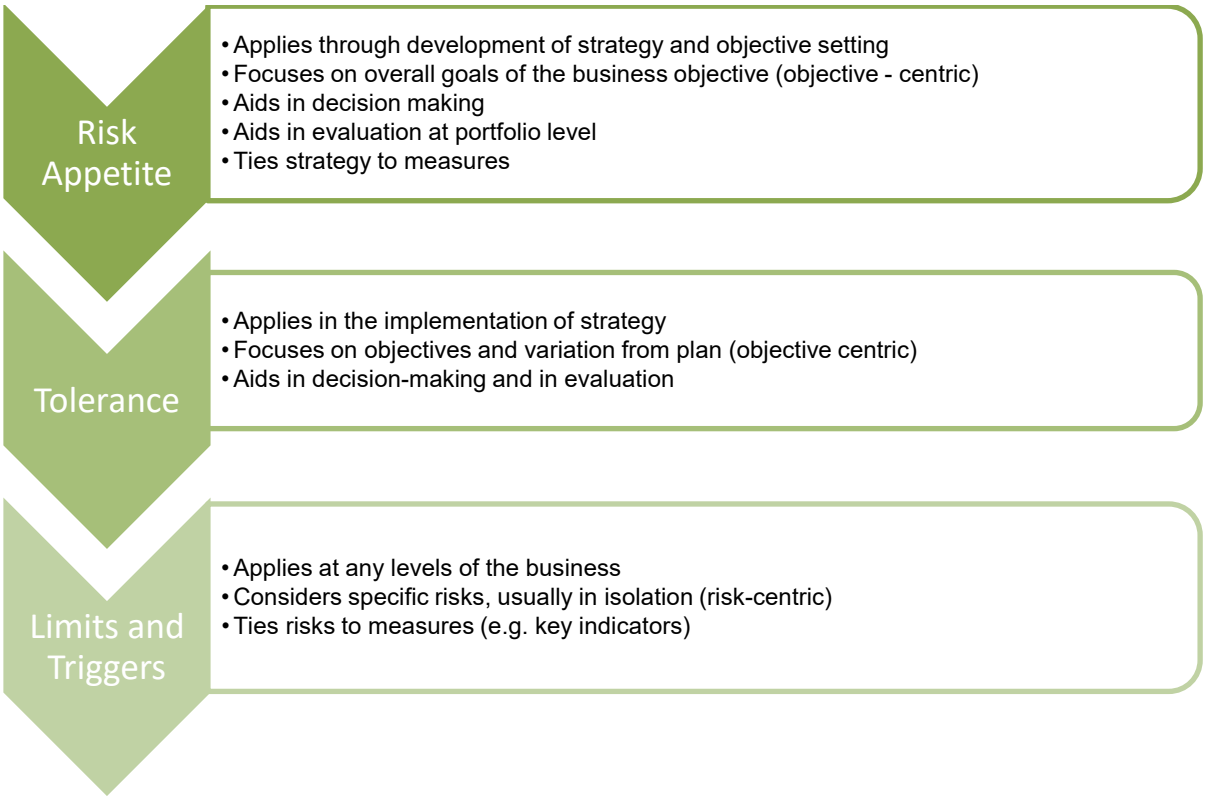


Figure 5. Risk Appetite, Tolerance and Limits

7. Risk Management Process

The risk management process comprises of the following elements (see figure below):

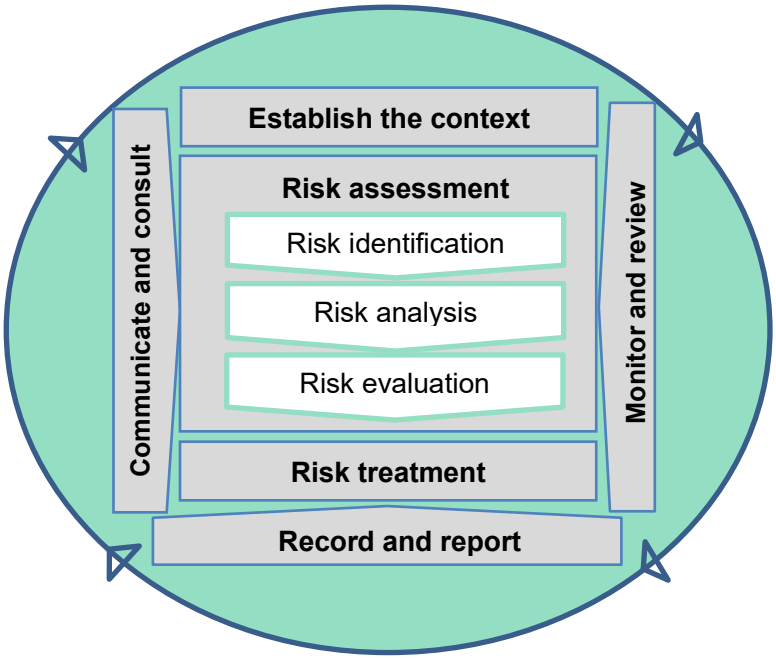


Figure 6. Risk Management Process

7.1 Communication and consultation

Communication and consultation with relevant internal and external stakeholders is to be undertaken at all stages of the risk assessment process to bring different areas of expertise together, ensure different views are appropriately considered, provide sufficient information to facilitate risk oversight and decision making and to build a sense of inclusiveness and ownership among those affected by the risk. It involves promoting awareness and understanding, as well as seeking feedback and information to support decisions made throughout the process.

Communication and consultation shall allow providing the risk management process participants with reliable and well-timed risk information, raising the level of awareness of risks, as well as methods and tools of responding thereto. The relevant information is defined, fixed, and produced in the form and within the term allowing employees to efficiently perform their functions.

Employees shall inform the risk manager of any risks occurred according to an internal document regulating record keeping and analysis of realised risks. For every risk realised, root causes of risk are analysed, and measures are taken to avoid such occurrence in the future.

Reporting of risks events is a non-threatening process, with no blame attached to those highlighting the occurrence of an event.

7.2 Establishing the scope, context and criteria

This part of the process is undertaken to gain an understanding of the purpose of the risk assessment and factors that may require consideration throughout the process. It includes establishing and defining the scope of the activity being assessed and associated boundaries of the risk assessment; the relevant objectives to be considered and any relevant relationships to other projects, processes and activities; desired outcomes from the steps to be taken; decisions that need to be made; the internal and external environment; resources required and associated responsibilities; risk assessment criteria, tools and techniques to be applied and records to be kept throughout the risk assessment process.

Figure 7. The relationship between our organisation's vision, strategies, policies and plans to our operations.

Your Activity or Business Plan should have business objectives that link to our strategies, policies and plans. Business objectives that do not align, or only partially align, to the strategy will not support the achievement of the mission and vision and may introduce unnecessary risk to our risk profile. That is, we may consume resources that would otherwise be more effectively deployed in carrying out other business objectives.

Setting business objectives clearly will also reveal links to internal and external stakeholders on whom you will rely as well as other internal/external factors that will impact your objectives.

7.3 Risk Identification

The risk assessment process starts by identifying risks that may impact strategy and business objectives (including project related objectives). We shall focus on identification of risks that have the following types of impacts:

- Risk 1 potentially impacts the strategy directly.
- Risk 2 impacts the organisation-level business objectives.
- Risk 3 impacts multiple business objectives that then aggregate and impact organisation-level business objectives.
- Risk 4 impacts a single business objective and that also impacts organisation-level business objectives.

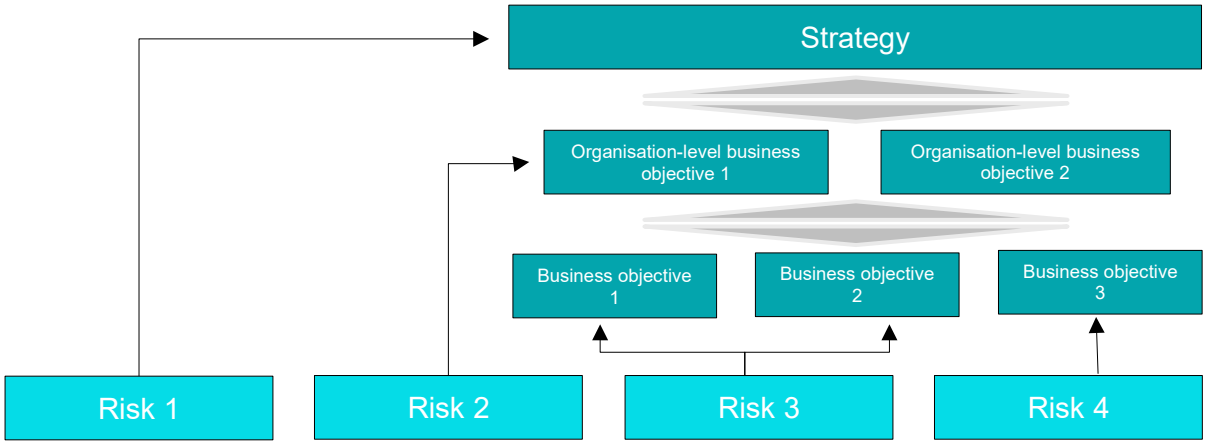


Figure 8. Risk impact types

In order to demonstrate comprehensive risk identification risks need to be identified across all functions and levels.

Various tools and techniques may aid to effectively gather risk information. Techniques might include (see Appendix 3. Risk Assessment techniques):

- Brainstorming - with team members, stakeholders, experts in the field;
- Examining historic incidents/projects/activities;
- Interviews – with subject matter experts, stakeholders, etc.

Questions to ask at identification and analysis include:

- When, where, why and how are the risks likely to occur, and who might be involved?
- What is the source of each risk?
- What are the impacts of the risk?
- What existing controls exist and are they adequate to mitigate the risk given the likelihood and impact?
- Who are the major stakeholders involved in the risk process?

The Project considerations (see Appendix 4.) can be used to help identify risks associated with Projects.

Project risks must be identified during the planning process, however can be added as and when necessary.

Once identified, risks are structured into meaningful risk statements. Risk statements can be described by using a standard sentence structure (see Appendix 5. Describing risks with Precision):

- The possibility of [describe potential occurrence or circumstance] and the associated impacts on [describe specific business objectives set by our organisation].

Example: The possibility of a change in foreign exchange rates and the associated impacts on revenue

- The risk to [describe the category set by our organisation] relating to [describe the possible occurrence or circumstance] and [describe the related impact].

Example: The risk to financial performance relating to a possible change in foreign exchange rates and the impact on revenue.

Questions and Answers

When should I seek to identify risks?

It is also beneficial to periodically take a fresh look at your risks and when formulating budgets and plans or embarking on a major new project are both great opportunities to review and evaluate.

Do I need to consider *everything* that could happen?

No. Like all government organisations, we have limited resources available to manage our risk. Therefore an important part of this exercise is to gain an understanding of the key risks – the ones that pose threats to the achievement of our objectives or unlock significant opportunities – so that we can best focus those resources. Consequently it is perfectly coherent to consciously consider a risk so remote as to be not worth recording. You are not expected to plan for literally every event.

Should I just consider 'what could go wrong'?

No. As noted in the definition of risk, a mistake often made is to focus on the 'negative threat' aspect and neglect the 'positive opportunity'. Although the mechanics of this framework deal principally with 'negative' risks, it is important that you consider these alongside potential opportunities.

What if I identify more risks than I can manage?

Firstly, it may be that many of the risks you have identified are already effectively managed by the day-to-day practice of your business. The next steps – evaluating and treating the risks – will help you in forming a picture of what risks genuinely present a need for 'extra' management. Secondly it might be that you have cast the net too wide on horizon scanning. Look again at the risks you have identified and consider, in reality, are they issues that will require attention in the near term or until the circumstances described are more likely to arise.

The time horizon used to assess risks should be the same as that used for the related strategy and business objectives.

7.3.1 Risk classification

The types of risks faced by our organisation:

- Strategic Risks are risks that affect or created by our strategy and organisation business objectives, as defined in the long term plan.
- Operational Risks are risks connected with the internal resources, systems, processes, and employees (including external contracted employees) or from external events, but is better viewed as the risk arising from the execution of an organisation's business functions.
- Project Risks are specific to the scope of the project and are often unique in nature and short term.

7.4 Risk analysis

Analysis involves developing an understanding of the risk, the likelihood of the risk occurring and the full range of potential impact/consequences, and determination of inherent risk severity, risk ownership, risk prioritisation and key risk indicators.

Exceptions to risk assessment

Safety and Wellness risks that have multiple reoccurrences (which may indicate a systematic issue, or an issue of high organisational importance) will be assessed in accordance with the criteria defined in this framework as a single risk. However, individual Safety and Wellness risks will be assessed and managed in accordance with the Health and Safety risk management system coordinated by People, Safety & Wellness business unit.

Risk analysis should be undertaken in the following steps:

7.4.1 Likelihood and impact scores determination

The likelihood and impact of identified risks are evaluated against a range of likelihood (probability) and impact (consequence) scores. The scores for each are given a numeric value of one through to five. The likelihood is an estimate of how likely the risk is to occur. The impact is an estimate of the effects of the risk if the risk manifested.

The assessment of likelihood and impact is mostly subjective, but can be informed by data or information gathered, audits, inspections, personal experience, institutional memory of previous events, insurance claims, surveys and a range of other available internal and external information.

The assessment of impact should be informed with reference to the highest scoring part of the risk i.e. if a risk scores 5 for financial impact but 4 for all other categories, the risk should be considered to have an overall impact score of 5.

The likelihood and impact scores along with criteria are demonstrated in Appendix 6. Likelihood table and Appendix 7. Impact table.

7.4.2 Inherent risk severity determination

Risks are assessed without taking into account the controls that currently exist to mitigate the risk.

The risk severity is determined by multiplying the Likelihood and Impact scores in a Risk Severity Matrix.

Risk severity = Likelihood x Impact

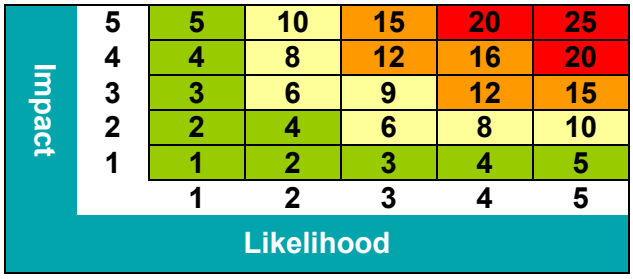


Figure 9. Risk severity matrix

7.4.3 Risk owner assignment

Each risk should be assigned a **Risk Owner.** For strategic risk the risk owner will be a member of the E-team. For operational risks the risk owner is often a subject matter expert, Business Unit Manager or Team Leader. For project risks the risk owner is most often the Project Manager or a subject matter expert.

The risk owner is accountable for managing the risk and reporting on the risk status. This involves communicating with treatment owners to ensure the treatments are current and remain effective, performing reviews of the risk assessment to ensure currency, identifying additional treatment requirements and closing the risk if it becomes redundant.

7.4.4 Risk prioritisation

Once risks have been assessed they can be mapped onto the prioritisation matrix. Inherent risk severity ratings are prioritized as either an Extreme, High, Moderate or Low risk. Extreme and High risks, along with risks that sit outside of risk appetite become the key risks that will be escalated for further actions discussed in sections 7.4.5.,7.5.,7.6. Risks that sit within risk appetite (typically moderate and low risks) should be periodically reviewed in case circumstances change, whereby the risk(s) are escalated for further actions.

Risk prioritisation matrix	
20-25	**Extreme Risk:** Review this level of risk against the Risk Appetite. Escalate for consideration to the E-team for further required actions.
12-16	**High Risk**: Review this level of risk against the Risk Appetite. Escalate for consideration to the E-team for further required actions.

6-10	**Moderate Risk**: Review this level of risk against the Risk Appetite and discuss with the Business Unit Manager or Project Manager. This level of risk will need to be monitored against the risk appetite and any changes should be reported to the Business Unit Manager.
1-5	**Low Risk**: Review this level of risk against the Risk Appetite and manage according to process and procedure. The risk should be monitored and any increase in risk should be reported to the appropriate risk coordinators.

Figure 10. Risk prioritisation matrix.

In case of equal severity of risks considering the availability of resources we must evaluate the trade-offs between allocating resources to mitigate one risk compared to another. The prioritisation of risks, given their severity, the importance of the corresponding business objective, and risk appetite will help our organisation in our decision-making. We must prioritise risks in order to inform decision-making on risk treatments and optimise the allocation of resources.

The following additional priorities could be used:

- Adaptability: The capacity of our organisation to adapt and respond to risks.
- Complexity: The scope and nature of a risk to our organisations success. The interdependency of risks will typically increase their complexity.
- Velocity: The speed at which a risk impacts our organisation. The velocity may move our organisation away from the acceptable variation in performance (see figure 5. Velocity)
- Persistence: How long a risk impacts our organisation.
- Recovery: The capacity of our organisation to return to tolerance. Recovery excludes the time taken to return to tolerance, which is considered part of persistence, not recovery.
- Performance; risks that affect performance levels approaching the outer bounds of tolerance may be given priority.

Score	Time of Risk Impact
1	There is time for correction.
2	Risk impact materialises with certain delay.
3	Risk impact materialises immediately.

Figure 11. Velocity

7.4.5 Key risk indicators

Key Risk Indicators (KRI), as defined in the Methodology of development and implementation of Key Risk Indicators, are among the principal tools of risk and risk sources monitoring. KRIs are indicators providing our organisation with early warnings of risk source changes in various areas of activity. KRIs allow identifying prospective risks and taking early measures to avoid

the realisation of risk and to minimise its impact on our organisation's activities, and shall be developed for the key risks.

7.5 Risk Evaluation

The evaluation process looks at the strength of the existing controls in place aimed at decreasing the likelihood of risk occurrence or the level of impact in the event of risk occurrence and determines whether residual risk severity is tolerable.

7.5.1 Existing controls

The effectiveness of existing controls to mitigate risk must be assessed based on the expert opinion of risk owner. The existing controls such as systems, procedures or practices aimed at modifying risk must be determined. Such controls may be management, technical, legal or procedural. A process (described in Promapp) must be reflected in the risk register if it exerts the intended or assumed modifying effect on risk i.e. reduce the likelihood and/or impact of a risk.

Common controls	
• Delegations • Committees • Reporting • Policies, procedures and guidance material • Qualifications • Insurance • Employment screening • Training and required learning • Code of conduct	• Reconciliations • Segregation of duties • Audits, reviews and investigations • Checklists, templates • Personal protective equipment • Physical access controls • IT firewalls • Passwords • Independent checks • Position descriptions

Figure 12. Common controls

Effectiveness	Description	Quantification
Effective	Control is mostly reliable, efficient and effective; will significantly reduce the risk likelihood and/or impact; fully documented processes and well communicated.	up to 99% effective
Somewhat effective	Control is somewhat effective; will have some effect on reducing risk likelihood and/or impacts; additional action required to improve existing controls and/or possibly implement some additional controls; improved documentation	up to 60% effective

	and/or communication of controls required.	
Ineffective	Control is not reliable, efficient or effective; will not reduce the risk likelihood and/or impact; reliable, effective and efficient controls to be developed and implemented; controls need to be documented and communicated.	0% effective

Figure 13. Control effectiveness rating

7.5.2 Residual risk severity tolerability

Residual risk severity is determined based on the outcome from analysis of control effectiveness rating and inherent risk severity. The effectiveness of existing controls for key risks will then be tested as per an annual internal audit plan.

Control effectiveness	**Residual risk severity**			
Effective	Low	Low	Low	Low
Somewhat effective	Low	Low	Moderate	Moderate
				High
Ineffective	Low	Moderate	High	Extreme
	Low	Moderate	High	Extreme
	Inherent risk severity			

Figure 14. Residual risk severity

If residual risk severity is not acceptable or tolerable then a risk treatment action plan must be developed as soon as practicable in accordance with section 7.6. A risk could be acceptable even in the following circumstances, including but not limited to:

- No treatment is available;
- The cost of applying the required treatment outweighs the impact or the benefit;
- The opportunities involved significantly outweigh the threats.

Authority of acceptance/ retention of residual risk severity outside of risk appetite lies with the CEO and/or the Council.

7.6 Risk treatment action plan

Risk Treatment action plan includes one or the combination of the following actions:

- Treat - additional control measures to reduce impact and/or likelihood.
- Tolerate - accept current level of risk.
- Terminate - ceasing to perform the activity causing the risk if possible.
- Transfer - transfer risk to third party generally by means of insurance or to another entity.

Depending on the activity or operation that is being assessed and the priority of the risk, risk treatment strategies can involve the development and implementation of long or short term risk treatment action plans (see risk treatment action plan template Appendix 8).

We must consider the potential costs and benefits of different risk treatment action plans. Generally, anticipated costs and benefits are commensurate with the severity and prioritisation of the risk. For example, a high-priority risk with a greater severity may warrant increased resource costs, given the anticipated benefits of the treatment action plan. The benefit of a risk treatment plan can be evaluated in the context of the achievement of strategy and business objectives. We acknowledge that some instance we are also responsible for risk treatments that address any regulatory obligations, which again may not be optimal from the perspective of costs and benefits, but comply with legal or other obligations.

Selecting one risk treatment may introduce new risks that have not been previously identified or may have unintended consequences. For instance, the risk of floods damaging the building was reduced by purchasing insurance; however, it may bring the risk of low cash flow or credit risk exposure given the deteriorating financial condition of insurance provider.

7.6.1 Risk treatment ownership assignment

For key risks a treatment owner must be assigned to monitor and update the treatment. The treatment owner communicates with the risk owner to provide updates on relevant changes.

7.7 Developing portfolio view

We must develop and evaluate a portfolio view of risks in the form of risk register to view risk profile from an organisational-wide, or portfolio perspective.

- A portfolio view allows the Council and the E-team to consider the type, severity, and interdependencies of risks and how they may affect performance. Using the portfolio view, we identify risks that are severe at the organisational level.
- Portfolio view – focus is on our organisation's strategy and business objectives. Greater integration supports identifying, assessing, responding to, and reviewing risk at the appropriate levels for decision-making. The Council and the E-team focus greater attention on the achievement of strategy while responsibility and management of business objectives and individual risks within the risk inventory cascade throughout our organisation.
- Using portfolio view helps our organisation to observe risk that:
    - Increase in severity as they are progressively consolidated to higher levels within our organisation.
    - Decrease in severity as they are progressively consolidated.

- Offset other risks by acting as natural hedges.
- Demonstrate a positive or negative correlation to changes occurring in the severity of other risks.

- Portfolio view allows the Management to determine whether our organisation's risk profile is within the overall risk appetite.

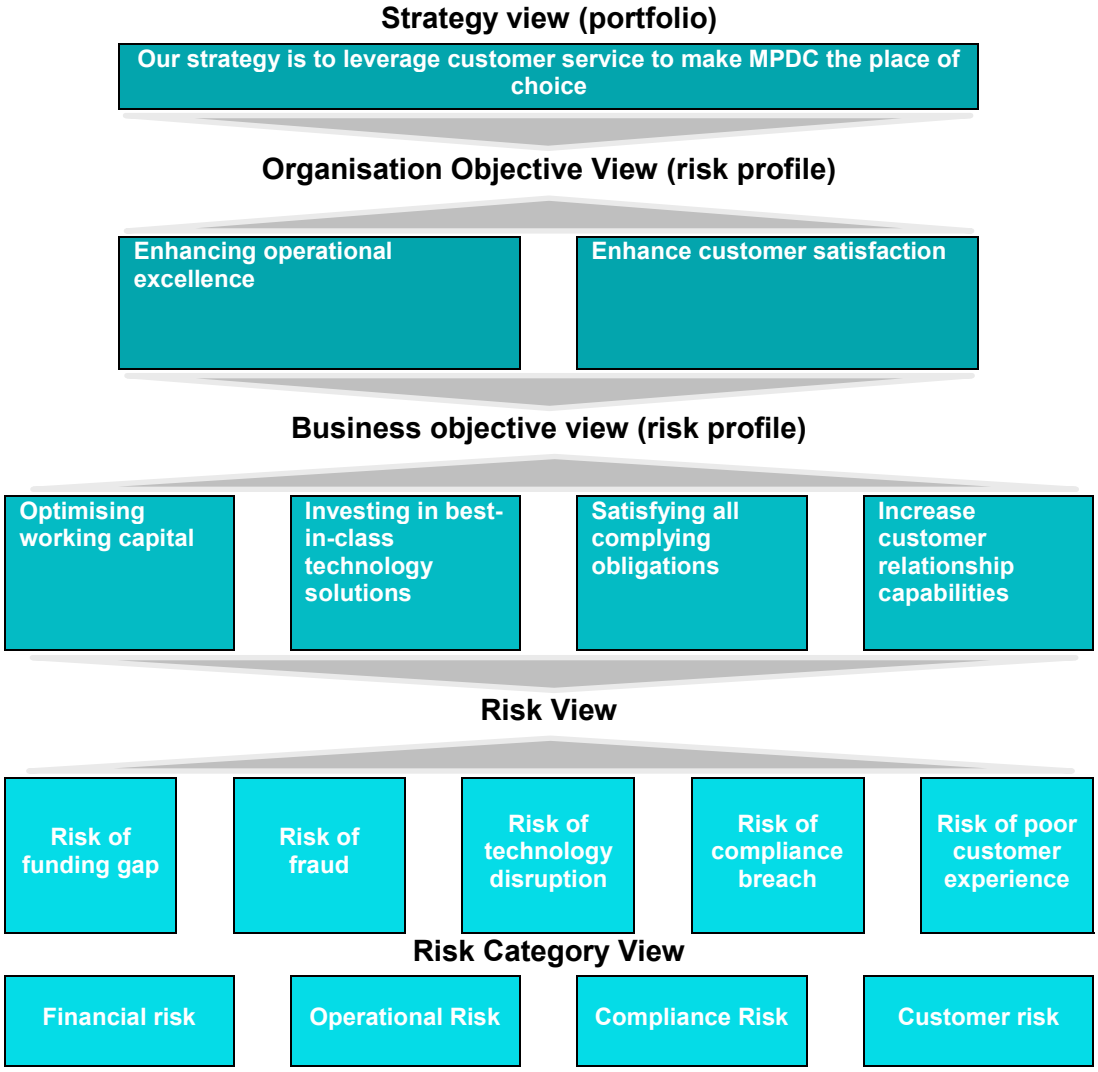


Figure 15. Portfolio View Concept

7.8 Monitoring and review

7.8.1 Substantial change assessment

Our organisation's strategy or business objectives and risk management practices and capabilities may change over time as we adapt to shifting business context. In addition, the business context in which we operate can also change, resulting in current practices no longer applying or sufficient to support the achievement of current or updated business objectives.

We identify and assesses changes that may substantially affect strategy and business objectives. Changes in internal and external factors related to the business context as well as changes in culture need to be identified.

We need to be aware of the potential for large, substantial changes that may occur, since such change may lead to new or changed risks, and affect key assumptions underpinning strategy.

We identify internal environmental changes related to the business context and changes in culture, such as (but not limited to): Rapid Growth, Innovation, Substantial changes in leadership and personnel, and external environmental changes related to the business context and changes in culture, such as (but not limited to) changing regulatory or economic environment.

The identified changes shall be reflected in the risk register during the regular revisions and update sessions.

7.8.2 Risk and performance review

If we determine that performance does not fall within its acceptable variation, or that the target performance results in a different risk profile than what was expected, we may need to:

- *Review business objectives:* we may choose to change or abandon a business objective if the performance is not achieved within acceptable variation.
- *Review strategy:* Should the performance result in a substantial deviation from the expected risk profile, we may choose to revise our strategy. In this case, we may choose to reconsider alternative strategies that were previously evaluated, or identify new strategies.
- *Review culture:* we may wish to review our culture and determine whether it is embracing the actions in a risk-aware manner.
- *Revise target performance:* we may choose to revise the target performance level to reflect a better understanding of the reasonableness of potential performance outcomes and the corresponding severity of risks to the business objective.
- *Reassess severity of risks:* we may reassess relevant risks, and results may alter based on changes in the business context, the availability of new data or information that enables a more accurate assessment, or challenges to the assumptions underpinning the initial assessment.
- *Review how risks are prioritised:* we may decide to either raise or lower the priority of identified risks to support reallocating resources. The change reflects a revised assessment of the prioritisation criteria previously applied.

- *Revise risk treatments:* we may consider altering or adding risk treatments to bring risk in line with the target performance and risk profile. For risks that are reduced in severity, we may redeploy resources to other risks or business objectives. For risks that increase in severity, we may reinforce risk treatments with additional processes, people, infrastructure, or other resources. As part of reviewing risk treatments, our organisation may also consider monitoring activities developed and implemented as part of internal control.
- *Revise risk appetite:* Corrective actions are typically undertaken to maintain or restore the alignment of the risk profile with our organisation's risk appetite, but can extend to revising it.

Corrective actions must align with the magnitude of the deviation in performance, the importance of business objective, and the cost and benefits associated with the changes in risk treatments.

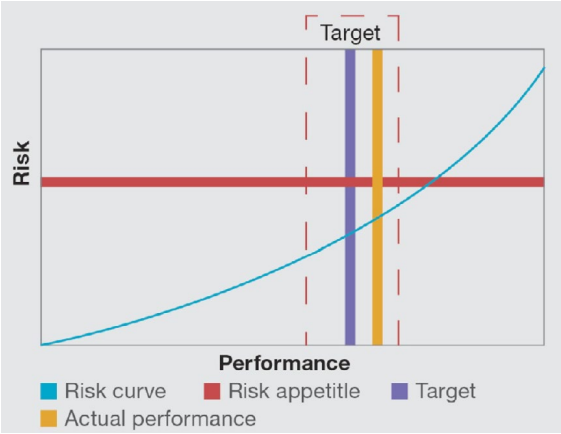


Figure 10. Risk Appetite, Tolerance and Actual performance.

7.8.3 Pursuing Improvement

Risk Management Framework will be reviewed on a minimum annual basis in order to ensure its conformity with the goals, scope and complexity of our organisation's activities, to consider cutting-edge risk management practices and accumulated experience.
The Management must pursue continual improvement throughout the organisation to improve the efficiency and usefulness of risk management practices at all levels.

7.9 Risk recording

We have developed a risk register template which can be found in Appendix 8. In accordance with the various levels of risk management across our organisation the following separate Risk Registers must be developed and maintained:

- Project Risk Registers – repository for recording and documenting identified project risks. Owned by the project managers or subject matter experts.
- Operational Risk Registers – repository for recording and documenting identified operational risks. Owned by the business unit managers.
- Key Risk Register – repository for recording and documenting key risks (strategic, operational and project risks). Owned by the risk manager.

7.10 Risk reporting

The outcomes of all steps of risk management process must be recorded and reported in the timeframe and format as outlined below:

Report to	Period	Content
Council	Annually (start of financial year)	• Risk appetite statement • Tolerances • Key risk register and Risk map • Risk treatment action plans on key risks • Information on any realised risks with indication of impact and the actions taken to remediate the impact and their effectiveness.
	6 monthly	• Key risk register and Risk map • Risk treatment action plans and implementation status • Information on any realised risks with indication of impact and the actions taken to remediate the impact and their effectiveness.
Audit & Risk committee	Annually	• Risk Improvement plan
	Quarterly	• Key risk register and Risk map • Key risk indicators status report • Risk treatment action plans on key risks and implementation status • Effectiveness of existing controls for key risks • Information on any realised risks with indication of impact and the actions taken to remediate the impact and their effectiveness.
E-team	Quarterly	• Key risk register and Risk map • Key risk indicators status report • Risk treatment action plans on key risks and implementation status • Effectiveness of existing controls for key risks • Performance variability and risk analysis • Information on any realised risks with indication of impact and the actions taken to remediate the impact and their effectiveness.

Appendix 1. Risk appetite scale

Risk appetite approach	Very High	High	Moderate	Low	Very low
Risk taking vs reward	We believe aggressive risk taking is justified	We are willing to take greater than normal risks	We take a balanced approach to risk taking	We take a cautious approach towards taking risk	We take caution and often accept as little risk as possible
Objective/negative impact relationship	Willing to accept a large negative impact in order to pursue strategic objective	Willing to accept some negative impact in order to pursue strategic objective	Potential negative impact and strategic objective completion given equal considerations	Only willing to accept a small negative impact in order to pursue strategic objective	Not willing to accept any negative impact in order to pursue strategic objective
Preferred risk treatment approach	Risk is accepted as much as Council permits	Preference to accept or reduce risk through internal measures	No preference towards risk treatment approaches	Preference to avoid risk or transfer it to an outside party or use secondary mechanism	Those risks that cannot be effectively treated or transferred are avoided
Risk treatment decision criteria	Minimum if any risk treatment actions are taken	Risk treatment actions are taken when a strong case can be made for cost effectiveness of potential outcomes	Risk treatment actions are made based on cost effectiveness, management priorities, and potential outcomes	Impact costs are given a relatively higher priority when risk treatment actions are considered	Risk treatment actions are taken even though prevention costs are greater than expected impact

Appendix 2. Types of risk sources

When identifying risks, all sources of potential risk should be considered. Some sources of risk are generic to all parts of the organisations. These include:

Risk breakdown Structure

RBS Level 0	RBS Level 1	RBS Level 2
MPDC Risk Guide	1 Finance and Economic Risks	1.1 Fraud
		1.2 Corruption
		1.3 Crime
		1.4 Business Continuity & Resumption
		1.5 Finance
		1.6 Commercial dealings
		1.7 Business issues
	2 Safety and Wellness risks	2.1 Design of H&S Risk Management System
		2.2 Level of implementation of H&S Risk Management System
		2.3 Technical: plant, process, substances, activities
		2.4 Human: culture, competence, communication
		2.5 Organisational: resourcing, contractors, procurement
		2.6 Environmental: geological, climate
	3 People and Wellness Risks	3.1 HR Management practices
		3.2 Recruitment
		3.3 Induction
		3.4 Training & Development
		3.5 Industrial Action
		3.6 EEO (equal employment opportunities)
	4 Legal Risks	4.1 Legal Relationships
		4.2 new legislation
		4.3 Changes to legislation
		4.4 Public Liability
		4.5 Crime
		4.6 Legal agreements
		4.7 Change of Government
	5 Reputation / Image Risks	5.1 Poor policy decisions
		5.2 Loss of corporate confidence
		5.3 Major challenge to council
		5.4 Illegal actions by employees
		5.5 Failure in finance system
	6.Environmental Risks	6.1 Natural Hazards
		6.2 Security
		6.3 Hazardous and Toxic Materials (e.g. chemicals, asbestos, gas etc)
		6.4 Public health (e.g. Legionella, food safety etc.)
		6.5 Emergency/ Disaster Management
		6.6 Environmental Management
		6.7 Waste and Refuse
	7.Operational Risks	7.1 Insurance
		7.2 Workers Compensation
		7.3 Information Technology/ Computer Systems
		7.4 Fleet
		7.5 Projects
		7.6 International Economics
		7.7 Market Competition
		7.8 Property and Physical Assets
		7.9 Technological Hazards

Appendix 3. Risk assessment techniques

In order to identify and assess risks, a combination of the following tools can be used (from ISO 31010 Risk management – Risk assessment techniques):

1) brainstorming – involves stimulating and encouraging free-flowing conversation about all potential risks and risk sources amongst a group of knowledgeable people, hindering the achievement of strategic goals and objectives, including the most unlikely, and subsequent selection of the most successful proposals.
2) structured/semi-structured interviews - in a structured interview, individual interviewees are asked a set of prepared questions from a prompting sheet, which encourages the interviewee to view a situation from a different perspective and thus identify risks from that perspective. A semi-structured interview is similar but allows more freedom for a conversation to explore issues that arise.
3) checklists - check-lists are lists of risks or control failures that have been developed usually from experience, either as a result of a previous risk assessment or as a result of past failures.
4) scenario analysis - can be used to identify risks by considering possible future developments and exploring their implications. Sets of scenarios reflecting ‘best case’, ‘worst case’, and ‘expected case’ may be used to analyse potential consequences and their probabilities for each scenario as a form of sensitivity analysis when analysing risk.
5) root cause analysis - attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms.
6) cause and effect analysis - is a structured method to identify possible causes of an undesirable event or problem. It organises the possible contributory factors into broad categories so that all possible hypotheses can be considered. The information is organised in a Fishbone diagram. Cause-and-effect analysis can be used as a method in performing root cause analysis.
7) questionnaires - a survey involving the collection of information according to a pre-compiled questionnaire.
8) bow tie analysis - bow tie analysis is a simple diagrammatic way of describing and analysing the pathways of risk from causes to consequences. The focus of the bow tie is on the barriers between the causes and the risk, and the risk and consequences. Bow tie diagrams are more often drawn directly from a brainstorming session. (Example of Bow tie diagram is illustrated in Appendix 10.).
9) analysis of internal and external statistical data - includes analysis of operational events database; results of inspections (reports of internal audit, external audit); experience of other local and foreign organisations (periodicals and reports of specialised agencies can be used).

The use of the above tools is determined based on the reasonability and rationality of use.

Appendix 4. Project considerations

Project name:	
Prepared by:	
Date:	
Governance	**Comments**
Legislative and corporate requirements, including approvals are identified, understood, straightforward and documented.	
Contractual and/or funding agreement obligations are identified, understood, straightforward and documented.	
Proposed form of contract for project delivery is agreed, understood, straightforward and documented (e.g. PPP, Turnkey)	
The impact on organisational procedures, process, policies or changes as a result of this project.	
Delivery	
Are employees and appropriate skills available to run the project, or deliver outcomes, post-completion?	
Is there a risk that a competitor may enter the market and impact service or feasibility of this project?	
Financial management	
Project funding vs estimated cost?	
The risk of any grant(s) for this project being Withdrawn is?	
Project budget has been completed to a high level of detail and is not based on cost plan only:	
Project cash flow has been established and approved	
A financial sensitivity analysis has been considered and documented	
Has the financial capacity of all contractors/consultants been formally investigated?	
Does the project require complicated or large amounts of security from the contractor(s)?	
Is the project subject to penalty clauses and potential damages payments?	
Reputation	
Could our performance on previous projects affect funding on this project?	
What is the community perception of this project?	
Political	
Is there a chance of a change in local government during the life of this project?	
Are there likely to be political timing pressures on this project ie. to bring forward or defer?	
Is there potential for this project to be affected by a change of priorities as part of Councils regular assessment of projects and priorities?	
Is there potential for this project to be impacted by community or lobby groups?	
Environmental	
Is there potential for environmental pollution of any kind from this project?	
Are there environmental risks if the project does not proceed?	
Are there sustainability or efficiency considerations that need to be factored into this project?	
Are there potential implications environmental legislative changes/requirements on this project?	

Safety and Wellness	
Have site safety assessments been undertaken?	
Does the project involve high risk activities that require licensing eg. asbestos, demolition, confined spaces?	
Are there issues of staff welfare on this project that need to be considered and addressed?	
Employees	
Is there a risk of loss of critical employees during this project?	
Is the Project team's time dedicated and adequate for this project?	
Have key contractors/consultants been individually identified and their time commitments/expectations on this project confirmed in writing?	
Projects	
The scope of the project is well defined and understood.	
The requirements of the project are understood and straightforward	
The project's major milestones and operational dates are known.	
The design of the project is finalised, understood and straightforward.	
Quality requirements of the project are understood?	
Products/technology being utilised is mature, widely used on previous projects and well researched and understood.	
Materials required are identified and readily available	
The method of tendering has been considered, agreed and approved by the Council?	
The tender evaluation panel and evaluation criteria has been considered, agreed and approved?	

Appendix 5. Describing risks with precision

Other considerations	Imprecise risk descriptions	Preferred risk descriptions
Potential root causes	• Lack of training increase the risk that processing errors and incidents occur • Low employee moral contributes to the risk that key employees leave, creating high turnover	• The risk that processing errors impact the quality of manufacturing units • The risk of losing key employees and turnover, impacting employees retention targets
Potential impacts associated with a risk occurring	• The risk of denial of service attacks due to legacy IT systems that result in leaked customer data, regulatory penalties, loss of customers, and negative press	• The risk of denial of service attacks impacting the ability to retain the confidentiality of customer data.
Potential effects of poorly implemented risk treatments	• The risk that bank reconciliations fail to identify incorrect payments to customers • The risk that quality assurance checks fail to detect product defects prior to distribution	• The risk of incorrect payments to customers impacting the entity's financial results • The risk of product defects impacting quality and safety goals

Precise risk identification:

- Allows the organisation to more effectively manage the risk inventory and understand its relationship to the business strategy, objectives, and performance.
- Allows the organisation to more accurately assess the severity of the risk in the context of business objectives.
- Helps the organisation identify the typical risk sources and impacts, and therefore select and deploy the most appropriate risk treatment plans.
- Allows the organisation to understand interdependencies between risks and across business objectives.
- Supports the aggregation of risks to produce the portfolio view.

Appendix 6. Likelihood table

Score	Descriptor	Qualitative	Quantitative
5	Almost certain	The event is expected to occur in most circumstances in the current environment; frequent past event history	90 – 99%
4	Likely	The event will probably occur in most circumstances in the current environment; some recurring past event history	70 – 89%
3	Possible	The event might occur at some time; some past warning signs or previous event history	30 – 36%
2	Unlikely	The event could occur at some time, no event history	10 – 29%
1	Rare	The event may occur but only in exceptional circumstances; no past event history	1 – 9 %

Appendix 7. Impact table

What could be the impact if the risk occurs?			Catastrophic 5 Critical event/circumstance with potentially disastrous impact on business sustainability	Major 4 Critical event or circumstance that can be endured with proper management	Moderate 3 Significant event or circumstance that can be managed under normal conditions	Minor 2 Event with consequences that can be readily absorbed but requires management effort to minimise the impact	Insignificant 1 Some loss but immaterial. Existing controls & procedures should cope with event or circumstance
Objectives	**Objectives**	Risks that have an impact on the performance	Key objectives in the LTP will not be achieved. Critical opportunity to innovate/improve performance missed/wasted Very difficult to recover from and possibly requiring a long term recovery period.	One or more key objectives in the LTP will not be achieved. Substantial opportunity to innovate/improve performance missed/wasted. Medium to long term effect and expensive to recover from.	Moderate impact on the success of the LTP. Good opportunity to innovate/improve performance missed/wasted. Medium term effect which may be expensive to recover from.	Minor impact on one or more activities	Insignificant impact on one or more activities
	Financial / Economic	Risks that have a financial impact on our organisation (revenue, expenses, assets, liabilities, reserve)	Loss of $2m or greater in any 12 month period	Loss $500k to $2m in any 12 month period	Loss $100k to $500k in any 12 month period	Loss $50K to $100k in any 12 month period	Loss less than $50k in any 12 month period
Project	**Project Budget**	Risks that impact the ability to deliver project outcomes within budget	Critical budget over-run; threat to viability of project	Significant budget over-run requiring allocation of significant funding and resources	Substantial budget over-run requiring additional funding and/or resources	Marginal budget over-run; manageable within contingency funding	Insignificant impact on budget manageable within allocated budget
	Project Timeframe	Risks that impact the ability to deliver project outcomes within timeframe	Critical over-run affecting many milestones; threat to ability to deliver critical project outcomes on time	Significant impact on project milestones; requiring review of implementation date	Substantial impact on project milestones; potential impact project delivery date	Marginal impact on project milestones, manageable within resources	Insignificant impact on project milestones

Appendix 8. Risk treatment action plan template

No	Risk statement	Risk sources	Residual risk severity	Risk treatment action plan	Resources required	Due date	Risk Treatment owners	Risk Owner	Completion form	Status	Comments	Target Residual risk severity
1	2	3	4	5	6	7	8	9	10	11	12	13

Appendix 9. Risk register template

No	Strategy of MPDC	Business objective	Type of business objective (organisational/ business unit)	Time horizon of business objective	Target and tolerance	Risk statement	Risk classification	Risk code	Risk sources	Type of risk source	Existing controls		Control effectiveness rating	Risk owner	Inherent risk severity (impact x Likelihood)	Residual risk severity	Time of risk Impact
											Preventive	Detective					
1	2	3	4	5	6	7	8	9	10	11	12		13	14	15	16	17

Appendix 10. Bow tie diagram